Univerza v Ljubljani

Fakulteta za računalništvo in informatiko

Večna pot 113, SI-1000 Ljubljana

MATJAŽ ŠKODA

Načrtovanje informacijsko-organizacijske varnosti v rastočem podjetju v fazah od zagonskega podjetja do zrele organizacije

MAGISTRSKA NALOGA

Mentor: prof. dr. Denis Trček

Ljubljana, avgust 2016

Zahvala

Iskreno se zahvaljujem mentorju prof. dr. Denisu Trčku za spodbudo pri izbiri tematike. Še posebej se mu zahvaljujem za vodenje in strokovno pomoč ter za vso vloženo energijo, saj je zaradi tega pričujoča naloga na veliko višjem nivoju tudi z uporabo primernih slovenskih izrazov za mnoge tuje strokovne izraze, ki v slovenskem jeziku nimajo splošno znanih prevodov.

Moji dragi Vesni se zahvaljujem za vso podporo in razumevanje v času ustvarjanja tega dela ter pomoč pri oblikovanju besedila.

Slavistki, ge. Zdenki Meglič se lepo zahvaljujem za končno lekturo in še zadnje popravke besedila.

KAZALO

KAZALO SLIK

KAZALO TABEL

SEZNAM KRATIC IN POJMOV

BYOD	Bring Your Own Device (prinesi svojo osebno napravo)
CRM	Customer Relationship Management (upravljanje odnosov s strankami)
CVE	Common Vulnerabilities and Exposures (baza ranljivosti programske opreme)
ERP	Enterprise Resource Planning (integriran poslovni informacijski sistem)
IKT	Informacijsko-komunikacijska tehnologija (angl. ICT)
IT	Informacijska tehnologija (angl. information technology)
IS	Informacijski sistem (angl. information system)
MDM	Mobile Device Management (upravljanje mobilnih naprav)
NVD	National Vulnerability Database (baza ranljivosti PO, deluje pod okriljem vlade ZDA)
PO	Programska oprema
SIP	Session Initiation Protocol (vzpostavljanje povezave)
SKD	Standardna klasifikacija dejavnosti
SSO	Single Sign On (enotna prijava)
SUIV	Sistem upravljanja informacijske varnosti (angl. information security management system, ISMS)

POVZETEK

Zadnja leta je veliko govora o varnosti in varnostnih politikah v organizacijah in tudi o varnosti na nivoju celotnih držav. Standardi in zakoni le stežka sledijo hitremu napredku na področju informacijsko-komunikacijske tehnologije (IKT). Od organizacij in držav se pričakuje, da bodo zagotavljale varnost svojih sistemov IKT in podatkov ter informacij, ki jih ti sistemi hranijo.

V magistrski nalogi v prvem delu predstavim terminologijo in stanje ključnih standardov na področju varnosti IKT. Opišem družino standardov ISO/IEC 27000 za vzpostavitev sistema za upravljanje informacijske varnosti (SUIV), ki ga je v skladu s smernicami moč vpeljati tako v zagonska podjetja kot tudi v velike organizacije. Za mnoge organizacije je neprekinjeno poslovanje ključ do rasti in obstoja na trgu, zato predstavim standarde na področju obvladovanja neprekinjenega poslovanja vključno z načrtom za obnovo IKT po morebitnem škodnem dogodku. Obvladovanje sprememb je v današnjem hitrem tempu pomemben proces, ki se ga organizacije premalo zavedajo. V nadaljevanju zapišem ključne korake za uspešno vpeljavo obvladovanja sprememb v organizacijah. Ključ za dolgoročno uspešno obvladovanje informacijske varnosti leži tudi v transformaciji organizacijske kulture v varnostno organizacijsko kulturo. V šestih točkah zapišem priporočilo za uspešno vpeljavo varnostno-organizacijske kulture.

V osrednjem delu naredim analize statističnih podatkov SURS za področje varnosti IKT v slovenskih podjetjih. Pregled obsega posledice varnostnih incidentov, formalne strategije za varno uporabo IKT, seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT, uporabo varnostnih pripomočkov ali postopkov, obseg uporabe (odprtokodne) programske opreme (PO) ter obseg uporabe prenosnih naprav v podjetjih. V okviru analize izdelam tudi orodje (CVE-analyzer) za pomoč pri analizi ranljivosti PO v povezavi z bazo NVD CVE. S pomočjo dobljenih podatkov in statistične analize preverim štiri hipoteze, vezane na posledice varnostnih incidentov IKT in uporabo odprtokodne PO.

V nadaljevanju opišem najpogostejše napake, ki nastanejo pri razvoju PO, in predstavim predloge, kako v procesu razvoja in vzdrževanja povečati varnost PO.

V zadnjem delu navedem znane statistične podatke s področja varnostnih incidentov po svetu in na osnovi tega zapišem dodatna priporočila za slovensko gospodarstvo.

Ključne besede: informacijska varnost, neprekinjeno poslovanje, kultura organizacijske varnosti, posledice varnostnih incidentov, obvladovanje sprememb, NVD CVE, zagonska podjetja, statistični pregled varnosti, slovenska podjetja.

SUMMARY

IT security and security policies in organizations as well as information security (IS) on the state level have been widely discussed in the last years. Standards and laws hardly keep up with the rapid progress in the field of information and communication technology (ICT). Organisations and states are expected to ensure the security and privacy of their ICT systems.

In the first part of this master's thesis, I present basic terminology and standards from the field of ICT security. I describe the ISO/IEC 27000 family of standards for introduction and management of information security management systems (ISMS), which can be in line with the guidelines implemented in start-up companies as well as in large organizations. For many organizations a business continuity is a key to growth and existence on the market. Bearing that in mind, I present the standards in the field of business continuity management, including ICT disaster recovery plan strategy for cases of disruptions. At todays rapid pace, change management is important process of which organizations are not sufficiently aware of. Further, I present key steps for successful implementation of change management into the organizations. The key to successful long-term management of IS is also in the transformation of the organizational culture into the security organizational culture. On the basis of simple six-step plan I make a recommendation for successful implementation of the security organizational culture.

In the central part of the thesis, I analyse statistical data collected by the Statistical Office of the Republic of Slovenia (SURS) related to ICT security in Slovenian enterprises. The review covers ramifications of ICT related security incidents, formally defined ICT security policies and reviews, informing of the staff of their obligations in ICT related issues, usage of internal security facilities or procedures, usage of (open source) software in enterprises and provision of portable devices with mobile Internet access by type and purpose in enterprises. In order to help me with the analysis, I also created a tool (CVE-analyzer) to help me with the analysis of software vulnerabilities according to data from NVD CVE database. On the basis of obtained data and statistical analysis I check four hypotheses related to ramifications of ICT related security incidents and the use of open source software in Slovenian enterprises.

Further on, I present the most common mistakes in software development process and introduce the proposals for increasing of software security in development and maintenance process.

In the last part, I introduce world-wide statistical data from the field of data security incidents and on their basis I propose additional recommendations for the Slovenian economy.

Key words: information security, business continuity, organizational security culture, security incidents, change management, NVD CVE, startup companies, statistical review of security, Slovenian enterprises.

1 Uvod

1.1 Namen

Zadnja leta je veliko govora o varnosti in varnostnih politikah v organizacijah in tudi na nivoju celotnih držav. Standardi in zakoni le težko sledijo hitremu napredku na področju informacijsko-komunikacijske tehnologije (IKT). Od organizacij in držav se pričakuje, da bodo zagotavljale varnost svojih sistemov IKT in podatkov ter informacij, ki jih ti sistemi hranijo. Vendar pa same varnostne politike in standardi, kot sta ISO/IEC 27002:2013 [40] in ISO22301:2012 [35], ne dosežejo svojega namena, če niso na pravi način 'vgrajeni' v delovne procese organizacije.

Namen naloge je prikazati različne poglede na varnost IKT. Najprej z vidika standardov in smernic ter napredka na tem področju, nato še z vidika statističnih raziskav glede na velikost podjetja in dejavnost, v kateri podjetje deluje.

1.2 Cilji

Ciljev te magistrske naloge je več. Prvi je podati ključna področja, ki jih je potrebno upoštevati pri uspešnem uvajanju organizacijske varnosti.

Drugi je na osnovi dostopnih statističnih podatkov podati primerjave glede na velikost podjetij (od malih do velikih podjetij) ter glede na dejavnost podjetij. Na osnovi ugotovitev bodo podane smernice in predlogi za izboljšave.

Tretji cilj je ugotavljanje, ali iz obstoječih statističnih podatkov o uporabi programske opreme lahko karkoli sklepamo o ranljivosti podjetij.

Rezultat magistrskega dela so smernice za zmanjšanje izpostavljenosti slovenskih podjetij. Podane so najbolj kritične skupine podjetij (število zaposlenih, panoga) ter ključne smernice, kako hitro izboljšati organizacijsko ter tehnično varnost glede na izkušnje podobnih podjetij po svetu.

S tem bo imelo magistrsko delo uporabno vrednost za podjetja v slovenskem prostoru, predvsem tista, ki želijo z nizkimi investicijami vzpostaviti ali izboljšati varnost sistemov IKT. Podane smernice in ugotovitve bodo lahko v pomoč tako zagonskim podjetjem kot velikim organizacijam.

1.3 Raziskovalno področje in metode

Če želimo podati dobre smernice za postavitev organizacijske varnosti, je potrebno poznati čim več dejstev o podjetju. Nekatera od njih so: velikost podjetja (število zaposlenih), panoga, v kateri podjetje deluje, ter kakšno programsko opremo uporablja.

Danes obstaja na tem področju že nekaj opravljenih statistik, na osnovi katerih bodo pripravljene smernice za slovenska podjetja. V magistrski nalogi je predstavljena tudi groba primerjava posledic incidentov v slovenskih organizacijah in organizacijah po svetu.

Metoda dela je temeljila na pregledu različne strokovne literature in spletnih virov, ki obravnavajo organizacijsko varnost. Pri tem sem pregledal spletne in ostale relevantne vire statističnih podatkov na področju informacijske varnosti. Del analize je bil opravljen na podlagi primerjave statističnih podatkov o uporabi programske opreme ter števila incidentov z javno dostopno bazo ranljivosti programske opreme NVD CVE [4], [65], [78].

2 Informacijska varnost

2.1 Osnovni pojmi

V nadaljevanju bodo pogosto uporabljeni naslednji izrazi, ki se pojavljajo na področju informacijsko–organizacijske varnosti, zato je prav, da jih podrobneje predstavim.

Varnost (angl. security)
Varnost lahko definiramo kot zmanjševanje ranljivosti sredstev (angl. assets) in virov (angl. resources). Po drugi definiciji varnost pomeni zaupnost, celovitost in razpoložljivost virov (povzeto po [17]).

Zasebnost (angl. privacy)
Zasebnost pomeni pravico do ohranjanja osebnih zadev in razmerij pred zunanjim svetom. Ključ do zagotavljanja zasebnosti je varnost. Seveda pa samo tehnologija ne more zagotavljati zasebnosti in mora biti zato ustrezno podprta z zakonodajo (povzeto po [17]).

Informacijski sistem (angl. information system)
Informacijski sistem je sistem (avtomatiziran ali neavtomatiziran), ki ga sestavljajo ljudje, tehnologija in procesi za zbiranje, prenos, razširjanje podatkov na načine, ki predstavljajo informacijo[1] uporabnikom [58].

Sredstva (angl. assets)
Za vzpostavitev varnostne politike moramo najprej določiti sredstva, ki jih bomo varovali, in kakšna je pomembnost določenih sredstev. Sredstva so lahko fizična (strežniki, računalniki, prenosne naprave, ...) ali pa neopredmetena (logična), kot so baze podatkov, intelektualna lastnina ipd. V organizacijah navadno sredstvom dodelimo lastnike (skrbnike), te pa združimo v skupine (vloge).

Grožnje (angl. threats)
Grožnje za informacijske sisteme so lahko človeške (heker, računalniški kriminalec ipd.), okoljske (električni udar, poplava, slabo fizično varovanje ipd.), lahko so naključne (kreativnost uporabnikov, zaposleni želijo opraviti svoje delo) ali načrtovane (gospodarsko vohunjenje, želja nekdanjega zaposlenega po maščevanju, napad s strani hekerske organizacije ipd). Grožnje, ki predstavljajo nevarnost za organizacijo, je mogoče ločiti tudi na notranje (npr. nezadovoljen zaposleni) in zunanje grožnje (npr. gospodarsko vohunjenje).

[1] Informacija izhaja iz podatkov, ki so surova dejstva o dogodkih ali fizičnem okolju. Podatek postane informacija, ko je obdelan/preoblikovan v takšno obliko, da ima pomen za človeka.

Ranljivost (angl. vulnerability)
Ranljivost je neželena lastnost sredstva. Če pride do izrabe (angl. exploit) določene ranljivosti s strani določene grožnje, gre posledično za varnostni incident.

Incident (angl. incident)
Incident je posledica izrabe ranljivosti sredstva s strani grožnje. Posledice incidentov so lahko velike ali majhne. Lahko pride do nedelovanja sistema, kraje zaupnih informacij, ogrožanja drugih sredstev ipd.

Tveganje (angl. risk)
Tveganje je ocena verjetnosti, da bo določena grožnja uspela izrabiti ranljivost sistema (sredstva). Glede na tveganja in vrednotenje vpliva sprejmemo kontrole za obvladovanje tveganj. Preostalo tveganje je tveganje, ki ostane po obravnavi tveganja.

Vpliv (angl. impact)
Vpliv je ocena, kako velike posledice bi lahko imel določen incident na delovanje organizacije. Ocena je lahko kvalitativna ali kvantitativna, lahko gre tudi za finančno oceno.

2.2 Standardi na področju upravljanja informacijske varnosti

Večina literature (tudi standard ISO 27001 [38]) definira upravljanje informacijske varnosti kot zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij:

- zaupnost - informacija je dostopna le pooblaščenim osebam oz. procesom;
- celovitost - ohranjena je pravilnost in popolnost informacijskega vira;
- razpoložljivost - informacijski vir je dostopen in uporaben za pooblaščene osebe, ko ga te potrebujejo.

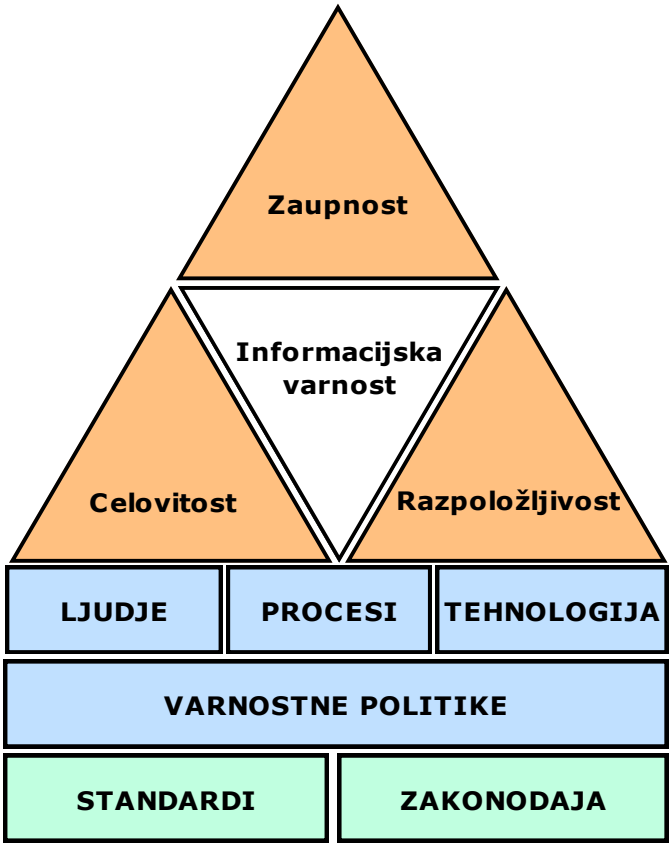
Poleg tega se pojavljajo še pojmi, kot so pristnost, nezatajljivost, integriteta in zanesljivost informacij. Vse to je potrebno za zagotavljanje upravljanja informacijske varnosti, vendar le-ta ne more obstajati brez ljudi, procesov in tehnologije, ki jih povezujejo in usmerjajo varnostne politike. Varnostne politike pa temeljijo na standardih in podpori zakonodaje (slika 1).

Ključni standard na področju upravljanja informacijske in organizacijske varnosti je danes ISO/IEC 27001:2013 [38], ki spada v družino standardov ISO/IEC 27000 za obvladovanje informacijske varnosti. Omenjene standarde sta pripravili Mednarodna organizacija za standardizacijo (v nadaljevanju ISO) in Mednarodna elektro-tehnična komisija (v nadaljevanju IEC).

Standard ISO/IEC 27001 se uporablja za vzpostavitev celovitega sistema upravljanja informacijske varnosti (SUIV)[2]. Opredeljuje model za vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema za upravljanje varovanja informacij. Standard predlaga procesni pristop in

[2] angl. Information Security Management System (ISMS)

opredeljuje osnovne aktivnosti, ki jih mora izvajati organizacija, da bo sistem upravljanja informacijske varnosti uspešen.



Slika 1: Piramida informacijske varnosti (vir: lasten)

Standard ISO/IEC 27001:2013 je nadgradnja standarda ISO/IEC 27001:2005, ki je nadomestil standard BS7799-2 (ta ni več v veljavi). Standard BS7799-2 je leta 1999 objavil Britanski inštitut za standardizacijo (British Standards Institute - BSI). Decembra 2000 je koda dobrih praks BS7799, ki je bila objavljena 1995, postala standard ISO/IEC 17799. Ta standard je bil posodobljen v letu 2005 in postal standard ISO/IEC 27002.

Standard ISO/IEC 27001 ima podobne zahteve kot standard ISO/IEC 17799, toda hkrati zagotavlja obvezne zahteve, ki morajo biti izpolnjene, da ima organizacija zagotovljen celovit pristop pri vpeljavi SUIV (vzpostavitev, vpeljava, delovanje, nadziranje, pregled, vzdrževanje in izboljševanje formaliziranih sistemov SUIV). Tako se zmanjšajo odvečne naložbe v ločene projektne skupine, kajti vpeljati je potrebno samo en standard.

Naštejmo še nekaj pomembnejših standardov, ki spadajo v družino ISO 27000:
ISO/IEC 27000 - uvod in pregled družine standardov SUIV;
ISO/IEC 27001 - specifikacija za vzpostavitev celovitega sistema upravljanja informacijske varnosti (SUIV);
ISO/IEC 27002 - kodeks prakse, predhodno znan kot ISO 17799 in BS 7799;
ISO/IEC 27003 - pomoč pri načrtovanju implementacije SUIV;

ISO/IEC 27005 - upravljanje tveganj v SUIV;
ISO/IEC 27006 - digitalni certifikati in registracija;
ISO/IEC 27004 - standard meritev za izboljšanje učinkovitosti SUIV;
ISO/IEC 27007 - revidiranje (angl. auditing) SUIV;
ISO/IEC 27008 - revidiranje varnostnega nadzora;
ISO/IEC 27010 - smernice za upravljanje z informacijsko varnostjo v medresorni in medorganizacijski komunikaciji;
ISO/IEC 27011 - informacijska varnost v telekomunikacijah;
ISO/IEC 27031 - smernice za pripravo IKT za neprekinjeno poslovanje;
ISO/IEC 27032 - kibernetska varnost;
ISO/IEC 27034 - aplikacijska varnost;
ISO/IEC 27035 - upravljanje z incidenti;
ISO/IEC 27037 - dokazi za postopek digitalne forenzike;
ISO/IEC 29147 - odgovorno razkritje ranljivosti.

Na sliki 2 vidimo seznam in relacije vseh standardov, ki spadajo v družino ISO 27000. Razdelimo jih na naslednje skupine:

a. standardi za pregled in terminologijo (ISO/IEC 27000);
b. standardi za zahteve (ISO/IEC 27000, ISO/IEC 27006);
c. standardi s splošnimi priporočili in postopki (ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC 27008, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27016);
d. standardi za priporočila glede na dejavnost organizacije (ISO/IEC 27010, ISO/IEC 27011, ISO/IEC TR 27015, ISO/IEC 27017, ISO/IEC 27799).

Podrobnejši opis naštetih standardov lahko bralec najde v [37].

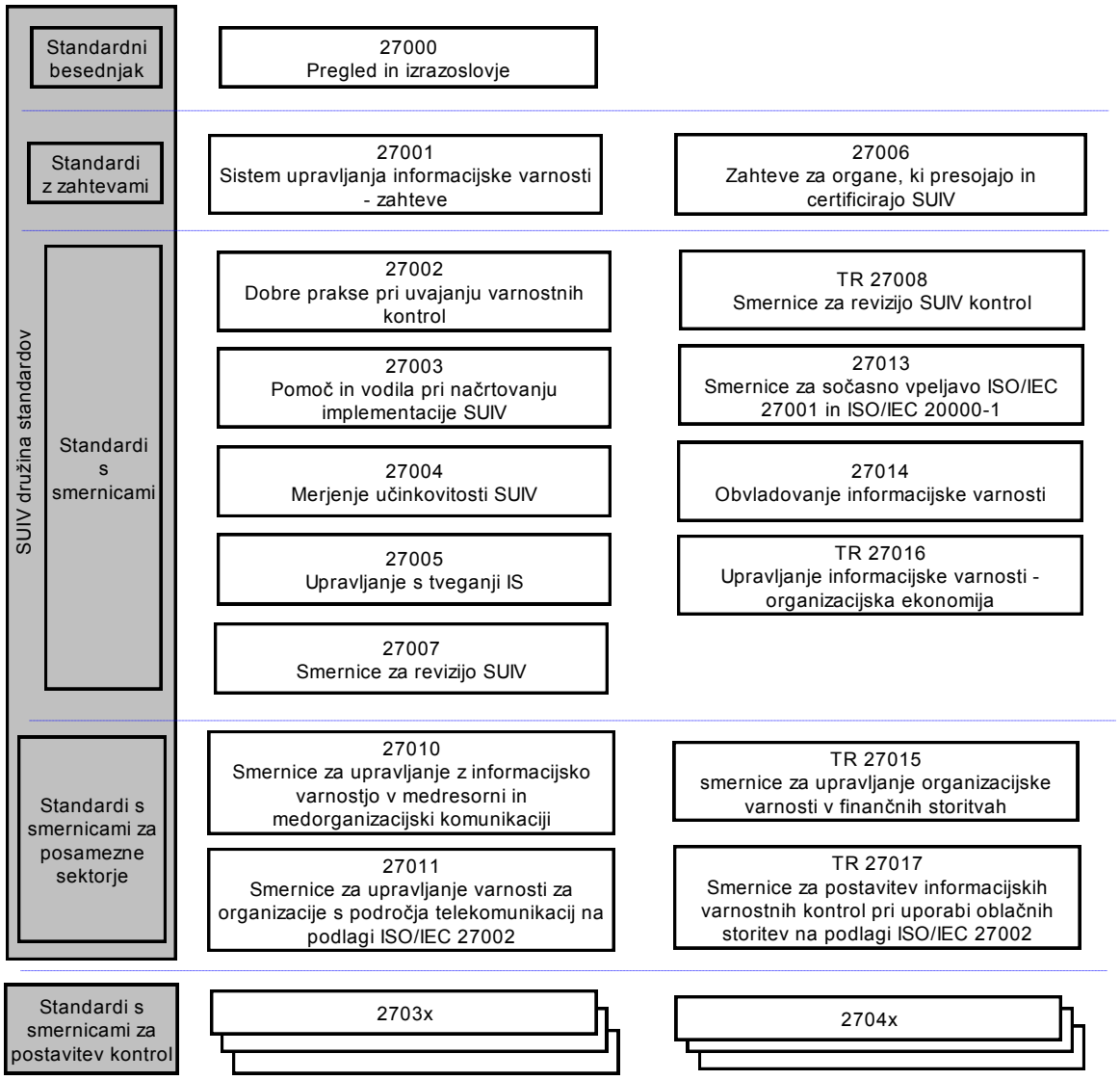
2.3 Opis standarda ISO/IEC 27001:2013

Standard ISO/IEC 27001:2013 daje velik poudarek implementaciji v okviru procesov organizacije in celotne strukture upravljanja (managementa) od zgoraj navzdol. Vodstvo organizacije mora izkazati zavezanost za vpeljavo s podporo in zagotavljanjem potrebnih virov za vpeljavo in upravljanje informacijske varnosti v organizaciji.

Standard ima deset kratkih klavzul:

1) področje uporabe standarda;
2) povezava z ostalimi standardi;
3) uporaba definicij in izrazov iz standarda ISO/IEC 27000;
4) okvir organizacije in zainteresirane strani;
5) vodenje informacijske varnosti in podpora vodstva;
6) načrtovanje SUIV; načrtovanje tveganj, odpravljanje tveganj;
7) podpora SUIV (viri, kompetence, zavedanje osebja, komunikacija, dokumentiranje);
8) delovanje SUIV (načrt delovanja in kontrola, načrtovanje tveganj, odpravljanje tveganj);
9) pregled izvedbe (spremljanje, notranji pregled, pregled s strani vodstva);

10) ukrepi za izboljševanje SUIV (odprava neskladnosti in ukrepi, neprestano izpopolnjevanje);
11) priloga A: Seznam kontrol in njihovi cilji.



Slika 2: SUIV (ISMS) družina standardov in njihove relacije (povzeto po: [37], str. 20)

Struktura standarda ISO/IEC 27001 je skladna z drugimi standardi, kot sta:

a) standard ISO/IEC 22301:2012 za upravljanje neprekinjenega poslovanja [35] ter
b) standard ISO/IEC 9001:2015 za upravljanje sistemov za vodenje kakovosti [28].

Organizacijam, ki želijo biti skladne z več standardi, skladnost standarda ISO/IEC 27001 z drugimi standardi olajša upravljanje njihove infrastrukture IKT z različnih zornih kotov. Pri tem gre za sinergijo, saj v delih, kjer se standardi prekrivajo, organizacije ne potrebujejo vlagati dodatnih naporov za izpolnjevanje vsakega izmed standardov.

Standardi ISO/IEC 27001:2005, ISO/IEC 22301:2012 ter ISO/IEC 9001:2015 predlagajo Demingov upravljalski krog "načrtuj-stori-preveri-ukrepaj" (slika 3), standard ISO/IEC 27001:2005 pa v nadgradnji na ISO/IEC 27001:2013 pušča organizacijam bolj proste roke pri izbiri enega od procesnih metodologij, kot je na primer tudi DMAIC 6-sigma [86].

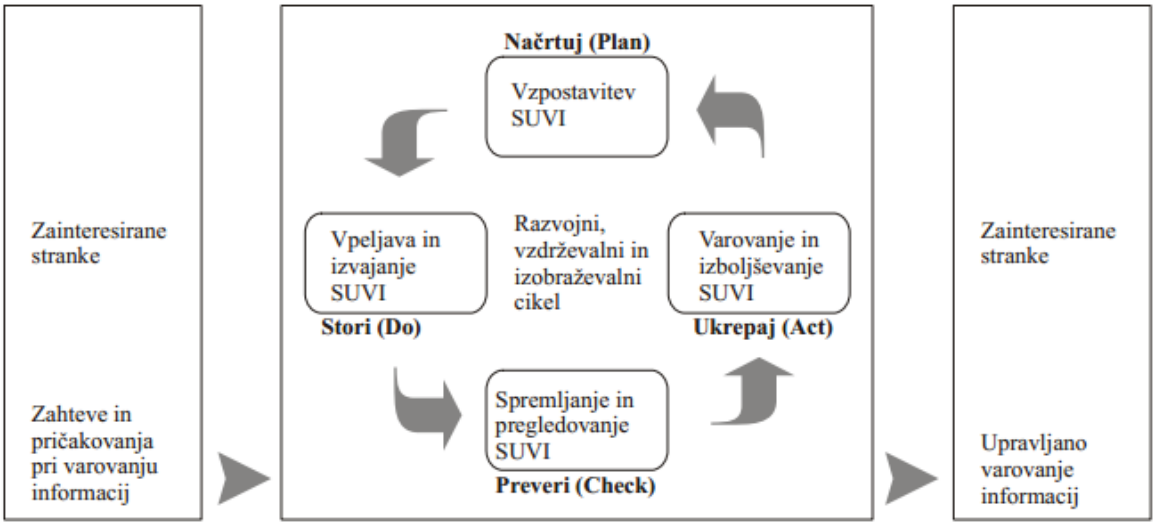
V nadaljevanju opišem posamezne korake Demingovega kroga (slika 3, povzeto po [39]):

Načrtuj: Vzpostavitev politike, ciljev, procesov in postopkov SUIV, ki so povezani s tveganjem in izboljšanjem varovanja informacij, z namenom zagotoviti rezultate v skladu s splošno politiko in cilji organizacije.

Stori: Vpeljava in delovanje politike, kontrol, procesov in postopkov SUIV.

Preveri: Ocenjevanje in kjer je izvedljivo, tudi merjenje delovanja procesov glede na politiko in cilje SUIV ter praktične izkušnje ter poročanje o dobljenih rezultatih vodstvu organizacije, da jih to pregleda.

Ukrepaj: Sprejetje popravnih in preventivnih ukrepov na podlagi rezultatov notranje presoje SUIV in vodstvenega pregleda, da se doseže neprestano izboljševanje SUIV.



Slika 3: Demingov upravljalski krog: načrtuj-stori-preveri-ukrepaj[3] za proces SUIV (vir: [39])

Nadgrajeni standard ISO/IEC 27001:2015 med drugim daje več poudarka zlasti varovanju podatkov in strojni opremi, medtem ko so bile nekatere kontrole, vezane na programsko opremo, osebje in omrežje, opuščene.

Pri vzpostavljanju standarda za upravljanje informacijske in organizacijske varnosti je priporočljivo vzpostaviti sprejemljiv nivo varnosti za podatke, programsko opremo in kategorije strojne opreme (vezano na kriterije za oceno tveganja).

[3] angl. Plan-Do-Check-Act (PDCA)

Dovolj poudarka je potrebno dati tudi zaposlenim ter klasifikaciji omrežja glede na potrebe in poslovno dejavnost organizacije.

Pomembno je omeniti, da je družina standardov ISO/IEC 27000 zastavljena tako, da jo lahko hitro vpeljemo v veliko oziroma katerokoli obstoječo organizacijo ali pa začnemo že v zagonski fazi podjetja, kjer v potrebnih okvirih vpeljemo osnovno upravljanje SUIV in ga potem z rastjo organizacije nadgrajujemo glede na potrebe organizacije.

2.4 Sistem obvladovanja neprekinjenega poslovanja (SONP)

Za mnoge organizacije je neprekinjeno poslovanje ključ do rasti in obstoja na trgu. Neprekinjeno poslovanje med drugim vključuje tudi zagotavljanje nemotenega delovanja informacijsko-komunikacijskih sistemov, kar od organizacije zahteva zmožnost, razpoložljivost, zanesljivost, vzdržljivost, varnost ter upravljanje procesov in ljudi tako, da je to doseženo.

Standard ISO/IEC 22301:2012 za zagotavljanje SONP določa zahteve za načrtovanje, vzpostavitev, vpeljavo, delovanje, nadzor, pregled, vzdrževanje in neprestano izboljševanje dokumentiranega sistema za upravljanje z namenom zaščite, zmanjšanja možnosti za incident, pripravo na odziv, odzivanje in okrevanje organizacije v primeru kritičnih dogodkov ([35], str 1).

Ta mednarodni standard podaja zahteve, potrebne za vzpostavitev in upravljanje sistema neprekinjenega poslovanja (SONP)[4]. SONP poudarja pomembnost ([35], str. V):

- razumevanja potreb organizacije in nujnosti vzpostavitve ciljev ter politik za upravljanje neprekinjenega poslovanja;
- vpeljave in delovanja kontrol ter meril za upravljanje sposobnosti odzivanja organizacije na moteče incidente (dejavnike);
- nadzora, pregledovanja uspešnosti in učinkovitosti SONP ter
- neprestanega izboljševanja SONP glede na cilje organizacije.

SONP ima podobno kot drugi sistemi za upravljanje naslednje ključne sestavine:

a) politiko;
b) ljudi z opredeljenimi odgovornostmi (vlogami);
c) proces upravljanja vezan na:
    1) politiko,
    2) načrtovanje,
    3) vpeljavo in delovanje,
    4) ocenjevanje uspešnosti,
    5) pregled s strani uprave/vodstva,
    6) izboljševanje;
d) dokumentiranje sprememb z revizijsko sledjo in
e) vpeljan katerikoli proces upravljanja neprekinjenega poslovanja, ki ustreza organizaciji.

[4] angl. Business Continuity Management System (BCMS)

Zahteve v standardu so splošne in namenjene vpeljavi v organizacije ne glede na njihovo velikost in področje delovanja. Obseg vpeljave teh zahtev je odvisen od okolja, v katerem organizacija deluje, in kompleksnosti organizacije. Cilj standarda ni postaviti strogo določenih struktur za vpeljavo SONP, temveč zadovoljiti zahteve organizacije glede na njene potrebe in obenem tudi zahteve vpletenih strank (kupcev, lastnikov, uprave, itd.). Te potrebe pa so oblikovane s pravnimi in regulatornimi okviri, zahtevami organizacije, zahtevami dejavnosti, v kateri organizacija deluje, proizvodi in storitvami organizacije, strukturo oziroma obliko organizacije ter zahtevami zainteresiranih strank.

Standard je namenjen vsem oblikam in velikostim organizacij, ki želijo:
a) vzpostaviti, vpeljati, vzdrževati in izboljševati SONP;
b) zagotavljati skladnost s politiko neprekinjenega poslovanja;
c) dokazati skladnost drugim organizacijam in posameznikom;
d) pridobiti certifikat skladnosti SONP.

Nekaj pozitivnih vplivov vpeljave SONP v organizacijo [96]:
- omejitev finančnih in operativnih posledic poslovnih motenj;
- prepoznana izražena tveganja in strategije, ki zmanjšajo ta tveganja;
- zagotovitev neprekinjenega poslovnega delovanja;
- ohranjanje stika s strankami in dobavitelji;
- vzpostavitev strategije za neprekinjeno poslovanje do izbranega nivoja in skrajšanje časa za okrevanje po morebitnem škodnem dogodku.

2.5 Načrt obnove po škodnem dogodku

2.5.1 Uvod

Vpeljava SUIV in/ali SONP organizaciji še ne zagotavlja nemotenega poslovanja ali uspešnega okrevanja po nepredvidenem škodnem dogodku.[5] V zvezi s tem velja pojasniti, da kot kritični incident oziroma škodni dogodek predpostavljamo poplavo, požar, cunami, potres, električni udar na sistemih IKT organizacije, uničenje vseh podatkov na strežnikih s strani zlonamerne hekerske organizacije ipd. Deloma so lahko ocene teh tveganj že zajete v politikah in kontrolah, sprejetih v SUIV. Vendar to ne zadostuje za hitro in uspešno okrevanje po takšnem škodnem dogodku.

Organizacije, kot so finančne institucije, zdravstvene institucije, procesni centri kreditnih kartic, spletne trgovine z velikim volumnom prometa (primer amazon.com), si ne morejo privoščiti izpada poslovnih sistemov IKT. Vsak takšen izpad za pet ali deset minut jih lahko stane na sto tisoče, morda milijone evrov. Takšna podjetja imajo zato običajno sisteme IKT zasnovane tako, da imajo popolno redundanco (podvojitev). To seveda ni poceni, vendar odtehta finančne izgube in zmanjšanje ugleda, ki bi ga povzročil izpad delovanja njihovih sistemov IKT.

[5] angl. disaster recovery (DR)

Povzeto po [47]: "*Obnova po škodnem dogodku je del zagotavljanja neprekinjenega poslovanja in se ukvarja s takojšnjim odzivom na takšen dogodek. V to kategorijo spada tako okrevanje izpada strežnika, varnostni vdor ali orkan. Okrevanje po škodnem dogodku ima običajno več jasno opredeljenih korakov v fazi vpeljave, vendar se ti koraki hitro zabrišejo v času krize, ker situacija skoraj nikoli ni takšna, kot je bilo predvideno. Načrt za okrevanje vključuje sanacijo posledic v najkrajšem možnem času in takojšen odziv za odstranitev vzroka in preprečevanje nadaljnje škode. To lahko vključuje izklop sistemov, ki so bili kompromitirani (hekerski vdor); oceno, kateri sistemi so uničeni zaradi poplave ali potresa; ter določitev najboljšega možnega načina za preprečitev nadaljnje škode. V neki točki se aktivnosti okrevanja po škodnem dogodku začnejo prepletati z aktivnostmi za neprekinjeno poslovanje (slika 4)*".

Slika 4: Cikel neprekinjenega poslovanja in načrta za obnovo po škodnem dogodku (povzeto po [47])

2.5.2 Standard ISO/IEC 24762 - načrt vzpostavitve neokrnjenega stanja po škodnem dogodku

V podpoglavjih 2.3 in 2.4 smo govorili o sistemu upravljanja z informacijsko varnostjo ter sistemu upravljanja neprekinjenega poslovanja. Omenili smo že, da sta standarda komplementarna in ju lahko vpeljemo v že obstoječo organizacijo ne glede na njeno velikost ali področje delovanja (od inovativnega zagonskega podjetja pa do zrele velike organizacije z več kot 250 zaposlenimi).

V ta namen se organizacije lahko oprejo na naslednje standarde:

- ISO/IEC 27031 - smernice za pripravo IKT za neprekinjeno poslovanje;
- ISO/IEC 27035 - upravljanje z incidenti;
- ISO/IEC 24762 - smernice za obnovo sistemov IKT po škodnem dogodku [36].

Ključni standard za pripravo načrta obnove po škodnem dogodku je ISO/IEC 24762:2008. Ta standard predpisuje smernice za vpeljavo, testiranje in izvajanje načrta za obnovo po škodnem dogodku in vključuje tako notranje kot zunanje (angl. outsourced) ponudnike storitev in infrastrukture za okrevanje IKT po škodnem dogodku. Standard zagotavlja smernice za:

- izvajanje, upravljanje, nadzor in vzdrževanje potrebne infrastrukture in storitev, potrebnih za obnovo po škodnem dogodku (tako kot je vpeljan sistem javnega opozarjanja osebja, naj zapusti stavbo, ali pa zahteva, da je vsa elektronska vrata mogoče odpreti ročno od znotraj);

- možnost preklopa na rezervni načrt ali podporo za obnovo sistemov IKT v organizaciji;
- zmogljivosti, ki jih morajo zagotavljati zunanji izvajalci za obnovo sistemov IKT, in priporočila, ki jim morajo slediti, da lahko zagotovijo varno okolje in infrastrukturo v času prizadevanja organizacije za obnovo po škodnem dogodku;
- izbor (rezervne) lokacije za obnovo (upoštevajoč dejavnike, kot so stabilnost okolja, dobra infrastruktura ipd.) in
- zahteve za ponudnike rezervnih lokacij po nenehnem izboljševanju kakovosti njihovih storitev.

V skladu s standardom ISO/IEC 24762:2008 je upravljanje neprekinjenega poslovanja sestavni del vsakega celovitega procesa obvladovanja tveganj in vključuje:

- prepoznavanje morebitnih nevarnosti, ki lahko škodljivo vplivajo na poslovanje organizacije in z njimi povezanih tveganj;
- zagotavljanje okvira za krepitev odpornosti na grožnje za poslovanje;
- zagotavljanje znanja ljudi, vodstva, zmogljivosti sistemov IKT, delovnih prostorov, postopkov, seznamov opravil, akcijskih seznamov itd. za učinkovit odziv na škodne dogodke in izpade poslovanja.

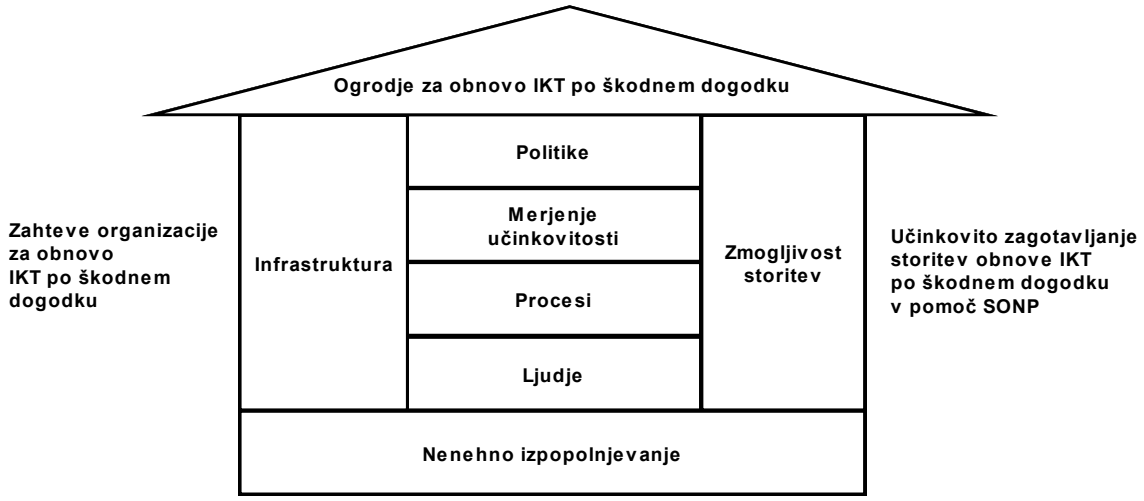
Standard ISO/IEC 24762:2008 temelji na večnivojskem ogrodju in obsega različne elemente pri zagotavljanju storitev IKT po škodnem dogodku (slika 5). Ključni nivo ogrodja, ki predstavlja pomemben vidik obnove storitev IKT po škodnem dogodku, sestavljajo politike, izvedba, merjenje učinkovitosti, procesi in ljudje. Ta nivo pomaga pri definiciji podporne infrastrukture in zmogljivosti storitev. Nivo nenehnega izpopolnjevanja predstavlja pristope, ki pomagajo izboljšati aktivnosti okrevanja IKT po škodnem dogodku in s tem dodaten nivo zagotavljanja kakovosti storitev.

"Politike" omogočajo ponudnikom storitev IKT po škodnem dogodku, da se usmerijo na (druga) področja, povezana s storitvami obnove IKT, in obenem omogočijo jasno obveščanje relevantnih strank glede zahtev, ki jih je mogoče izpolniti z zmogljivostmi ponudnika storitev obnove IKT.

"Merjenje učinkovitosti" omogoča ponudnikom storitev obnove IKT, da preučijo in izboljšajo svoje storitve ter obenem ponudnikom storitev zagotavlja sredstvo, da dokažejo, da njihove storitve izpolnjujejo zahteve organizacije.

"Procesi" zagotavljajo, da bo tudi na drugih področjih storitev obnove IKT sprejet skladen pristop, ki bo omogočal trajno vzdrževanje nivoja storitev in lažje usposabljanje osebja, ki opravlja storitve obnove IKT.

Termin "ljudje" se nanaša na skupino usposobljenih in dobro obveščenih ponudnikov storitev, organizacijo, in če je relevantno, tudi osebje tretjih oseb, ki je potrebno za delovanje, podporo in vzdrževanje praks obnove IKT. Obenem sta tudi varnost in dobro počutje osebja vidika, za katera bodo morali ponudniki storitev obnove IKT poskrbeti.



Slika 5: Ogrodje načrta za obnovo IKT po škodnem dogodku (povzeto po [36])

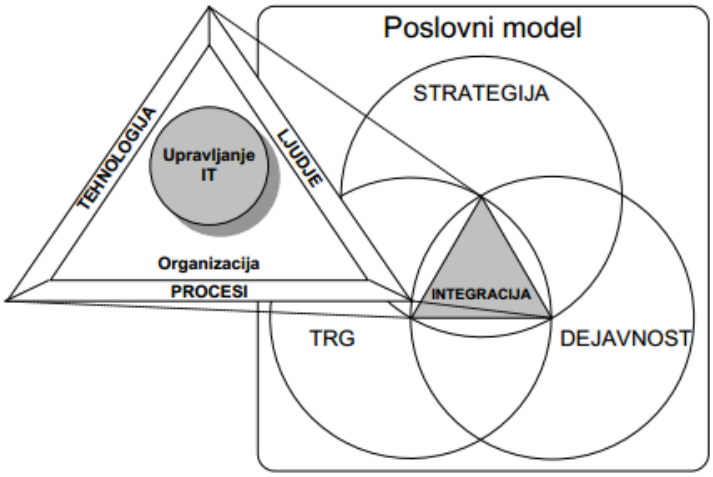
Standard ISO/IEC 24762 za implementacijo zahteva vpeljana standarda ISO/IEC 27001 in ISO/IEC 27002. S tem ima organizacija že ocene tveganj in pripravljene varnostne politike ter kontrole. Priporočljivo je upoštevati še standarda ISO/IEC 27031 in ISO/IEC 27035. Standard ISO/IEC 22301:2012 je komplementaren in je lahko predhodno vpeljan ali pa ne – odvisno od zahtev same organizacije.

2.6 Obvladovanje sprememb

2.6.1 Obvladovanje sprememb v IT

Predpisi (v prejšnjih poglavjih omenjeni standardi in tudi drugi) zahtevajo, da morajo biti spremembe poslovnih funkcij dokumentirane in da imajo revizijsko sled. Temu rečemo nadzor sprememb, ki prinaša večjo stopnjo stabilnosti poslovnim funkcijam in zahteva od osebja, da dokumentira in koordinira predlagane spremembe na sistemih, za katere je odgovorno. S tem, ko postaja ta proces bolj avtomatiziran, se pomembnost prenese od kontrole osebja k skladnosti s predpisi.

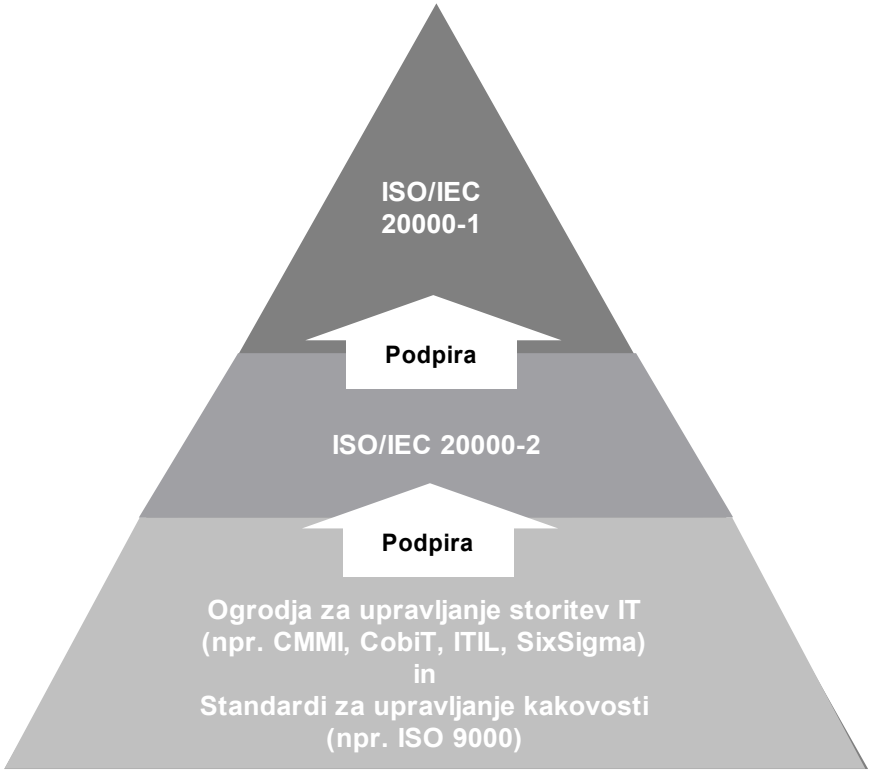
Primer politike upravljanja sprememb z opisanimi kontrolami za spremembe lahko bralec najde v [76]. Pomembnost obvladovanja sprememb v IT je že leta 2006 dobro povzel Krajnc [6]: *"Celovito upravljanje informacijskih sistemov in IT storitev postaja vedno bolj pomemben del celotnega upravljanja organizacij. Gre predvsem za usklajeno upravljanje poslovnih zahtev ter potreb osnovne dejavnosti, ki jih mora informacijski sistem organizacije v kar največji meri podpirati. V okviru celovitega upravljanja IT osrednjo vlogo igra upravljanje sprememb, ki mora združevati vse vidike in vire, ki vstopajo v proces spreminjanja. Od učinkovitosti upravljanja sprememb je namreč odvisno, ali bodo storitve IT izvajane brez prekinitev in brez nepredvidenih izpadov ali pa bo zaradi slabega in nenadzorovanega uvajanja sprememb uporabnikom treba pojasnjevati, zakaj neka storitev ni bila na razpolago. Zaradi tega je treba v okviru celovitega upravljanja IT v organizaciji zagotoviti oziroma oblikovati dobro pripravljen in skrbno načrtovan sistem upravljanja sprememb, ki mora združevati vse deležnike, vključene v proces upravljanja sprememb."*



Slika 6: Umestitev storitev upravljanja IT v okvire organizacije (vir: Krajnc [6])

Na sliki 6 je prikazano, na kakšen način lahko v splošnem umestimo upravljanje IT glede na dejavnost organizacije, trg, na katerem organizacija posluje ter strategijo poslovanja.

Pri vpeljavi celovitega upravljanja IT sta organizacijam v pomoč standard zahtev ISO/IEC 20000-1 (upravljanje storitev – sistemske zahteve) [32], ISO/IEC 20000-2 (smernice za uporabo sistemov za upravljanje storitev) [33] ter ogrodja za vpeljavo upravljanja s storitvami IT, kot so ITIL [74], CobiT in podobni. Na sliki 7 vidimo, da lahko tem standardom in ogrodjem pridružimo tudi družino standardov za obvladovanje kakovosti ISO/IEC 9000 in druge podobne standarde.

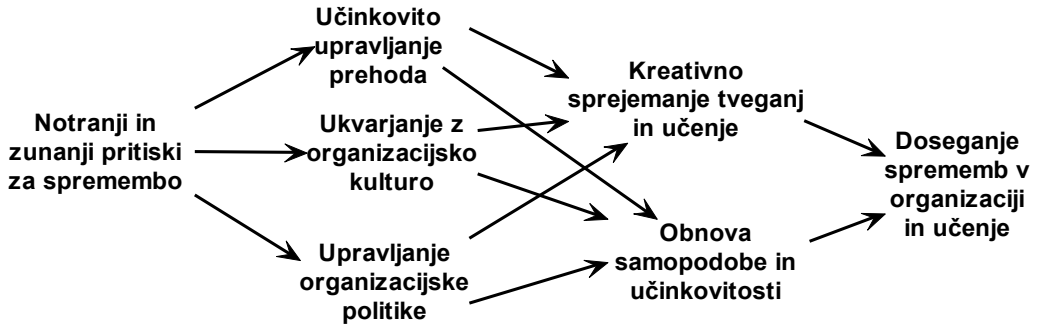


Slika 7: Relacije med ISO/IEC 20000 standardoma 1 in 2 ter SUIV ogrodji (povzeto po [45])

2.6.2 Kako uspešno vpeljati obvladovanje sprememb v organizacijo

Učinkovito obvladovanje sprememb ni koristno le zaradi skladnosti s standardi, temveč omogoča tudi agilnejši odziv organizacije na spremembe na trgu, povečuje dodano vrednost in tudi zadovoljstvo zaposlenih.

Zaradi vpetosti storitev IT v vse procese organizacije je smiselno, da obvladovanje sprememb vpeljemo ne samo na nivo osebja in oddelka IT, temveč v celotno organizacijo. Pri tem se je potrebno zavedati, da je upoštevanje organizacijske kulture eden od ključnih faktorjev za uspešno uvedbo in obvladovanje sprememb tako v IT oddelku kot tudi v organizaciji kot celoti. To je leta 1990 objavil že Carnall [23] (povzeto po [22]). Kljub temu, da Carnall daje v ospredje vodstveno (managersko) vlogo pred samim procesom sprememb, njegov nazor predstavlja pomembno vlogo pri postavitvi kontrolnega seznama za uspešno uvedbo sprememb (slika 8).



Slika 8: Obvladovanje prehodov upravljanja v organizacijah (povzeto po [22])

Pri uvedbi organizacijskih sprememb je potrebno v začetni fazi premostiti tri glavne težave. Prva je pritisk na zaposlene zaradi prevelikega števila sprememb naenkrat, ki ga je v raziskavi, ki jo je leta 2013 opravil Katzenbach Center, kar 65% vprašanih izpostavilo kot problem [20]. Obenem je 48% vprašanih kot razlog za neučinkovitost novo uvedenih sprememb navedlo pomanjkanje sposobnosti znotraj organizacij, ki bi zagotovile, da se novo vpeljane spremembe ohranijo in ne zvodenijo. Zato je za organizacije pomembno, da vlagajo v poslovne spremembe, izobražujejo in usposabljajo svoje zaposlene, da ti lahko čim prej implementirajo uvedene spremembe pri vsakodnevnem delu. Tretja težava je, da so ponavadi organizacijske spremembe načrtovane na vodilni ravni, z malo prispevka tistih na nižjih ravneh v organizaciji. Posledično je kar 44% vprašanih v raziskavi izjavilo, da niso razumeli, katere spremembe naj bi bile izvedene, 38% pa jih je navedlo, da se z vpeljanimi spremembami v podjetju ne strinjajo.

DeAnne Aguirre in Micah Alpern sta objavila tudi 10 smernic za uspešno obvladovanje sprememb v organizacijah, da bi se te lahko izognile zgoraj navedenim težavam [20].

1. **Vodenje v skladu s kulturo (organizacije)**
   Pri uvajanju sprememb je pomembno, da je v procesu implementacije sprememb upoštevana tudi obstoječa kultura znotraj organizacije, saj bodo tako zaposleni spremembe lažje sprejeli. Zato je pomembno, da vodilni znotraj organizacijske kulture v podjetju identificirajo elemente, ki so usklajeni s

predlaganimi spremembami, in te elemente v procesu uvedbe sprememb čim bolj poudarjajo.

2. Začeti je potrebno pri vrhu (vodstvu organizacije)
Kljub temu da je v uvedbo organizacijskih sprememb pomembno vključiti vse zaposlene, se vse uspešne uvedbe sprememb v organizaciji začnejo pri vrhu. Pomembno je, da se vodstvo organizacije uskladi glede načina uvedbe sprememb in ustvari skupno vizijo za razvoj organizacije ter v procesu implementacije deluje usklajeno.

3. Vključite vsa področja
V proces uvedbe sprememb je potrebno vključiti zaposlene na vseh nivojih oziroma strokovnih področjih, saj se zaposleni zaradi lastnega sodelovanja pri načrtovanju in uvajanju organizacijskih sprememb bolj aktivno angažirajo v procesu uvajanja sprememb.

4. Naredite primer racionalen in čustven hkrati
Vodstvo organizacije organizacijske spremembe običajno upravičí s strogo ekonomskimi cilji (vstop na nove trge, 20% rast ipd.), vendar se takšni razlogi zaposlenih čustveno ne dotaknejo. Zato je pomembno, da vodstvo pri uvajanju sprememb zaposlene tudi čustveno nagovori z dejanji, ki so pri zaposlenih pozitivno sprejeta (npr. vodstvo se iz luksuznih pisarn preseli v "open-space" in si tam delovni prostor deli z ostalimi zaposlenimi).

5. Delujte v smeri načrtovanih sprememb
Vodstvo je običajno prepričano, da bodo zaposleni po sprejemu novih pravil in smernic kar naenkrat spremenili svoje delovanje, vendar v praksi uvajanje sprememb ni tako enostavno. Zato je pomembno, da vodstvo jasno definira spremembe v delovanju, ki jih pričakuje od zaposlenih, ter te spremembe tudi samo implementira v praksi.

6. Delujte, delujte, delujte
Pomembno je, ne le da vodstvo spremembe ob začetku implementacije sporoči zaposlenim, temveč jih mora znova in znova sporočati zaposlenim, pri tem uporabljati različne komunikacijske načine ter spremembe tudi samo vpeljati v praksi.

7. Vodite izven okvirov
Pomembno je, da so v uvedbo organizacijskih sprememb poleg formalnega vodstva vključeni tudi zaposleni, ki imajo močan neformalen vpliv znotraj organizacije in jih zaposleni zelo spoštujejo oziroma cenijo.

8. Uporabite formalne rešitve kot vzvod
Prepričevanje zaposlenih, naj spremenijo svoje ravnanje, ne bo uspešno, če formalni elementi organizacijskih sprememb (kot je struktura, sistem nagrajevanja, usposabljanja ipd.) niso jasno definirani.

9. Uporabite neformalne rešitve
Tudi če so formalni elementi jasno definirani, to samo po sebi še ne zagotavlja uspešne uvedbe sprememb. Zato je pomembno, da se formalne rešitve uporabljajo v kombinaciji z neformalnimi rešitvami. Neformalna rešitev je lahko npr. sprememba slogana ali vizualne podobe organizacije.

10. Naredite oceno in se prilagajajte
Veliko organizacij naredi pri uvajanju sprememb napako, da v procesu implementacije sprememb uspeha ne ocenjuje sproti oziroma v določenih fazah. Če se proces implementacije sproti ocenjuje, je namreč po potrebi mogoče prilagajati naslednje korake v procesu in tako doseči maksimalen rezultat novo vpeljanih organizacijskih sprememb.

3 Kultura organizacijske varnosti

3.1 Uvod

Že v začetku osemdesetih let prejšnjega stoletja so raziskave pokazale, da organizacijska kultura lahko pomembno vpliva na uspeh in dobičkonosnost organizacije.

Uttal [52] organizacijsko kulturo definira kot skupne vrednote in prepričanja, ki medsebojno vplivajo na strukture in kontrolne sisteme znotraj organizacije z namenom oblikovanja (primernih) vedenjskih norm.

Za organizacijo je pomembno, da v svojo organizacijsko kulturo na pravi način umesti tudi varnost. Prav s tem pristopom bo organizacija lažje, bolj samoiniciativno in kontinuirano s strani zaposlenih vzdrževala in gradila proces organizacijske varnosti.

Potrebno se je namreč zavedati, da navkljub vsem tehničnim varnostnim in nadzornim sistemom pomembno vlogo pri izvajanju varnosti in varnostnih politik igra prav vèdenje in odnos osebja do varnosti v organizaciji.

Na temo organizacijske varnosti obstaja nešteto knjig, gradiv in člankov. Malo med njimi pa jih obravnava organizacijsko varnost kot kulturo organizacije. Z raziskavo, kako se varnostna organizacijska kultura razlikuje od navadne organizacijske kulture, se je v svojem članku ukvarjal Jo Malcolmson. Kot rezultat svoje raziskave o varnostni kulturi v organizacijah [9] je zapisal naslednje: "Varnostna kultura je skupek predpostavk, vrednot, stališč in prepričanj, ki jih imajo člani organizacije o tem, kako njihovo vedênje in ravnanje lahko vpliva na varnost organizacije".

V svoji raziskavi se ni osredotočil le na IT področje, temveč na splošna gospodarska področja, zato so njegove ugotovitve uporabne tudi v drugih dejavnostih, kot so proizvodnja, oskrba z električno energijo, zdravstvo ipd.

3.2 Kako uspešno vpeljati varnostno-organizacijsko kulturo

Medtem ko se male organizacije (zagonska podjetja) v obdobju po ustanovitvi večinoma osredotočajo na svojo rast, se ob uspešni tranziciji v srednjo ali veliko organizacijo srečajo z vprašanji varovanja svojega znanja, sistemov IKT, patentov, blagovnih znamk itd. Načeloma so takšne organizacije zelo agilne in hitro prevzamejo zdravo varnostno-organizacijsko kulturo, prav tako kot so verjetno od samega začetka prevzele metodologijo vitkega razvoja (angl. lean startup) [42], ki jim je v veliki meri olajšala uspeh in preboj na trgu.

Kot sem zapisal že v uvodu tega dela, ima kultura organizacijske varnosti lahko velik vpliv na dejansko izvajanje in izpopolnjevanje varnostnih politik in procesov. Toda, kako vpeljati kulturo organizacijske varnosti v srednje ali veliko podjetje, ki ni raslo v tem duhu od samega začetka?

Trček in Likar v svojem znanstvenem članku [16] predstavljata agilno in tudi v praksi potrjeno metodologijo MIS^2 (angl. "mee-square") oziroma metodo za integrativno varnost informacijskih sistemov (angl. method for integrative information systems security), ki na sistematičen način pomaga vzpostaviti upravljanje IKT tveganj in posledično na osnovi pristopa k reševanju le-tega obenem pomaga organizaciji narediti tranzicijo od splošne organizacijske kulture h kulturi organizacijske varnosti.

Metoda MIS^2 predlaga naslednjih šestih korakov:

1. Identificiranje udeležencev v MIS^2 metodi: V organizaciji je potrebno najti zaposlene, ki imajo dovolj znanja o sistemih IKT, in prav tako tudi tiste, ki so večinoma samo uporabniki IKT storitev in niso preveč dobro seznanjeni s podrobnostmi delovanja sistemov IKT.
2. Izbor sodelujočih v MIS^2 metodi: Izmed vseh možnih udeležencev izberemo tiste, ki so bolj inovativni in znajo razmišljati izven okvirjev (angl. thinking out of the box).
3. Seja kreativnega razmišljanja: Del izbrane populacije iz točke 2. naj strokovnjaki s področja IKT varnosti podučijo o osnovah varnosti, ne da bi zahajali v preveč tehnične podrobnosti, in jih spodbudijo h kreativnemu razmišljanju. V tej fazi kreativnega razmišljanja naj udeleženci ugotovijo tveganja in predlagajo potencialne rešitve.
4. Tehnična evalvacija: Za evalvacijo tveganj in predlaganih rešitev razdelite populacijo IKT strokovnjakov, tako kot predlaga 2. korak. Izmed njih izberite najbolj kreativne, ki imajo hkrati tudi znanje o IKT podrobnostih. Zraven je koristno povabiti tudi nekaj udeležencev iz 2. koraka. Ta skupina naj nato predlagane rešitve skupine iz 3. koraka oceni glede na možnosti za tehnično izvedbo.
5. Finančna in organizacijska evalvacija: Rezultati iz 4. koraka se posredujejo IT poslovodstvu podjetja za evalvacijo ekonomske izvedljivosti in v preverjanje, ali so ti rezultati skladni s strateškimi usmeritvami organizacije. Pomembno je, da se osredotočimo na največ tri najbolj resne grožnje naenkrat.
6. Implementacija: Vpeljite sprejete ukrepe in periodično (redno) ponavljajte te postopke, pri čemer sistematično sledite

implementaciji. S tem organizacija lahko zazna dodatne šibke točke, ki jih je še potrebno odpraviti.

Menim, da ima ta proces prav zaradi 6. koraka, ki narekuje redno sistematično ponavljanje celotnega postopka, pozitiven vpliv na krepitev organizacijske varnostne kulture, saj udeleženci več in ciljno komunicirajo o svojih opažanjih in zaznavajo pomanjkljivosti v IKT varnosti ter predlagajo možne rešitve. Hkrati se to znanje in zgoraj opisan postopek na podlagi neformalne komunikacije pozitivno širi tudi med ostale zaposlene v organizaciji.

Splošno varnostno zavedanje preide v varnostno kulturo takrat, ko se ljudje začnejo zavedati, da so varnostne kršitve nesprejemljive za okolje, v katerem delujejo [44]. To pa je namen pravilne uvedbe varnostne organizacijske kulture.

4 Statistični pregled varnosti v slovenskih organizacijah

4.1 Uvod

V tem poglavju prikazujem stanje in trende na področju varovanja ter uporabe informacijsko-komunikacijske tehnologije (IKT) v slovenskih podjetjih na osnovi statističnih podatkov SURS [90].

Pojem informacijsko-komunikacijska tehnologija (IKT) se nanaša na proizvode in postopke, ki se uporabljajo za shranjevanje, zapisovanje in druge vrste obdelav informacij. Dandanes se izraz IKT nanaša na informacijsko-komunikacijske tehnologije, ki so se razvile iz telekomunikacijske in računalniške industrije. Pojem IKT pa zajema tudi širši nabor izdelkov na področju telefonije, bibliotekarstva in drugih praks o filmih, faksih, revijah, člankih...[6]

Večina raziskav je bila nazadnje narejena med leti 2009 in 2012, vendar tudi iz njih dobimo določeno sliko in trende, ki jih lahko smiselno apliciramo na sedanje stanje na tem področju. Tako kot je dejal že Winston Churchill v svojem znanem citatu: »*Dlje kot lahko pogledamo v preteklost, dlje v prihodnost lahko vidimo.*«[7]

V nadaljevanju bodo obravnavani naslednji statistični podatki iz raziskav, ki se nanašajo na slovenska podjetja:

1. Posledice varnostnih incidentov, s katerimi so se srečala podjetja v 2010.
2. Formalne strategije za varno uporabo IKT z načrtom za njihov redni pregled v 2010, 2015.
3. Seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih 2010.
4. Uporaba internih varnostnih pripomočkov ali postopkov v podjetjih v letu 2010.
5. Obseg uporabe programske opreme IKT v podjetjih v letu 2011.

[6] Vir: https://sl.wikipedia.org/wiki/Informacijsko-komunikacijska_tehnologija.
[7] "The farther back you can look, the farther forward you are likely to see." - Winston Churchill.

6. Dodelitev prenosnih naprav z mobilnim dostopom do interneta v letu 2012.

Podjetja v statističnih tabelah so po velikosti klasificirana po naslednji klasifikaciji:

mikro podjetja: do devet zaposlenih;
mala podjetja: 10-49 zaposlenih;
srednja podjetja: 50-249 zaposlenih;
velika podjetja: 250+ zaposlenih.

V nekaterih tabelah se pojavijo naslednje oznake, zato prilagam njihov pomen (vir: SURS):
- ni pojava,
... ni podatka,
z zaupno,
M manj natančna ocena - previdna uporaba,
N za objavo premalo natančna ocena.

Na osnovi statističnih podatkov bom prikazal določene trende, ki se pojavijo z rastjo organizacije. Poleg tega bom izpostavil nekatere značilnosti podjetij, ki delujejo v posameznih dejavnostih.

Preveril bom tudi naslednje hipoteze:

H1: Če slovensko podjetje deluje v kategoriji velikih podjetij, potem je bolj ranljivo od mikro, malih in srednje velikih slovenskih podjetij.

V poglavju 4.2.3 bom naredil analizo števila posledic varnostnih incidentov med slovenskimi podjetji glede na vrsto dejavnosti po standardni klasifikaciji dejavnosti (SKD) [89], v kateri podjetje deluje. S tem bom poskušal ugotoviti, ali v Sloveniji obstajajo dejavnosti, v katerih so podjetja na področju varnosti IKT bolj izpostavljena. Glede na statistične podatke o posledicah varnostnih incidentov bom preveril naslednje raziskovalno vprašanje [75].

RV2: Ali porazdelitve posledic incidentov slovenskih podjetij kažejo na to, da vrsta dejavnosti glede na SKD, v kateri ta podjetja delujejo, lahko vpliva na število incidentov?

Več kot 64% slovenskih podjetij uporablja odprtokodne spletne brskalnike (vir: SURS [90]). Na osnovi podatkov o ranljivostih PO bom v procesu analize s pomočjo podatkov iz baze CVE določil, kateri spletni brskalnik je varnejši (po številu in po teži ranljivosti). Na tej osnovi bom v petem poglavju preveril naslednji hipotezi.

H3: Slovenska podjetja, ki uporabljajo odprtokodne spletne brskalnike, so bolj ranljiva od slovenskih podjetij, ki uporabljajo izključno licenčne spletne brskalnike.

H4: Če (slovensko) podjetje uporablja odprtokodno programsko opremo, potem je zaradi napak v tej opremi varnostno bolj izpostavljeno kot (slovensko) podjetje, ki uporablja izključno licenčno programsko opremo.

Hipotezi H3 in H4 podrobneje obravnavam petem v poglavju, kjer predstavim rešitev CVE-analyzer (priloga 1), ki sem jo ustvaril v okviru tega dela z namenom tehničnega ocenjevanja ranljivosti programske opreme. S pomočjo CVE-analyzerja in analize zbranih ranljivosti NVD-CVE [78] bom na primerih prikazal, kako je možno oceniti stopnjo ranljivosti posamezne programske opreme ali sklopa programske opreme.

4.2 Posledice varnostnih incidentov, slovenska podjetja v letu 2010

4.2.1 Pregled statističnih podatkov

Razlaga pojmov

Nedosegljivost storitev IKT zaradi napada od zunaj:
DDoS – Distributed Denial of Service attack (zavrnitev storitve) - napad od zunaj, ki onemogoči uporabo informacijskega sistema za uporabnike. Strežnik, omrežje je zasičen, obremenjen s toliko povpraševanji, da jih ne more obdelati, in je lahko zaradi preobremenitve začasno onesposobljen. DDoS je izboljšava DoS napada s tem, da DDoS prihaja iz porazdeljenih virov (strežnikov) in ga je težje preprečiti kot DoS.

Phishing - poskus pridobivanja informacij, kot so npr. gesla, uporabniška imena in podatki o kreditnih karticah s pomočjo e-pošte, ki usmeri uporabnika na lažne spletne strani.

Pharming - neposredni napadi na strežnik DNS ali na datoteko o gostiteljih, ki se nahaja na uporabnikovem računalniku. Pri tem so uporabniki, ne da bi to sploh vedeli, preusmerjeni na neprave spletne strani, čeprav v naslovno vrstico brskalnika pravilno vnesejo URL naslov strani, ki bi jo radi obiskali. Ker so lažne strani največkrat popolne kopije originalnih, uporabniki ne opazijo, da se nahajajo na lažnem naslovu, in oddajo svoje osebne informacije.

Zlonamerno spreminjanje podatkov – neželena sprememba podatkov, izbris podatkov (nameren, nenameren), selektivni izbris podatkov (dnevniške datoteke) z namenom zakrivanja sledi, delno uničenje podatkov zaradi okvare strojne opreme, nepooblaščeno spreminjanje podatkov ipd.

V letu 2010 so napake v programski ali strojni opremi povzročile nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov v 6,7% podjetij. V 2,5% podjetij so bili podatki uničeni ali popačeni zaradi okužbe z zlonamerno programsko opremo ali zaradi nedovoljenega dostopa (tabela 1).

V 1,7% podjetij je bila nedosegljivost storitev IKT posledica napada od zunaj, v 1,4% podjetij pa je prišlo do razkritja zaupnih podatkov v elektronski obliki s strani zaposlenih oseb (namerno ali nenamerno).

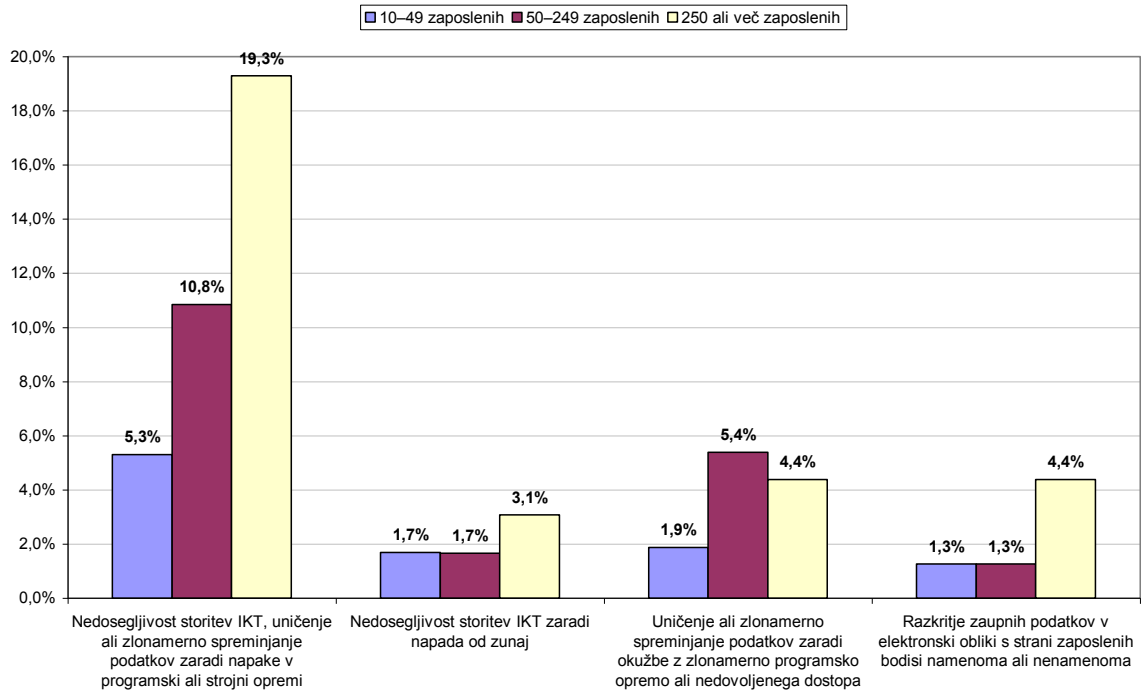
S posledicami varnostnih incidentov, povezanih s sistemi IKT, so se v letu 2009 najpogosteje spopadala velika podjetja, in sicer največkrat (19,3%) z nedosegljivostjo storitev IKT, uničenjem ali zlonamernim spreminjanjem podatkov zaradi napake v programski ali strojni opremi. Med srednje velikimi podjetji je bilo največ takih, ki so se spopadala s posledicami uničenja ali zlonamernega spreminjanja podatkov zaradi okužbe z zlonamerno programsko opremo ali zaradi nedovoljenega dostopa (5,4%).

Tip incidenta	Povprečje: 10 ali več zaposlenih	Mala podjetja: 10–49 zaposlenih	Srednja podjetja: 50–249 zaposlenih	Velika podjetja: 250 ali več zaposlenih
Število podjetij	7417	5925	1264	228
TI1: Nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi	6,7%	5,3%	10,8%	19,3%
TI2: Nedosegljivost storitev IKT zaradi napada od zunaj	1,7%	1,7%	1,7%	3,1%
TI3: Uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa	2,5%	1,9%	5,4%	4,4%
TI4: Razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma	1,4%	1,3%	1,3%	4,4%
TI5: Razkritje zaupnih podatkov zaradi vdora, 'pharming' ali 'phishing' napadov[8]	0,1%	z	-	z

Tabela 1: Posledice varnostnih incidentov, s katerimi so se srečala podjetja v letu 2010, po velikosti podjetja (vir: SURS)

Oznaka "-" pomeni "ni pojava", kar v nadaljevanju kvantitativno lahko upoštevamo kot vrednost 0. Oznaka "z" v tabeli pomeni zaupen podatek, ki s strani SURS ni objavljen in ga zato v nadaljnji analizi ne morem upoštevati.

[8] Zaradi zaupnih (oznaka z) in s tem nedosegljivih podatkov v TI5 teh podatkov ne bom uporabil pri nadaljnjih analizah.



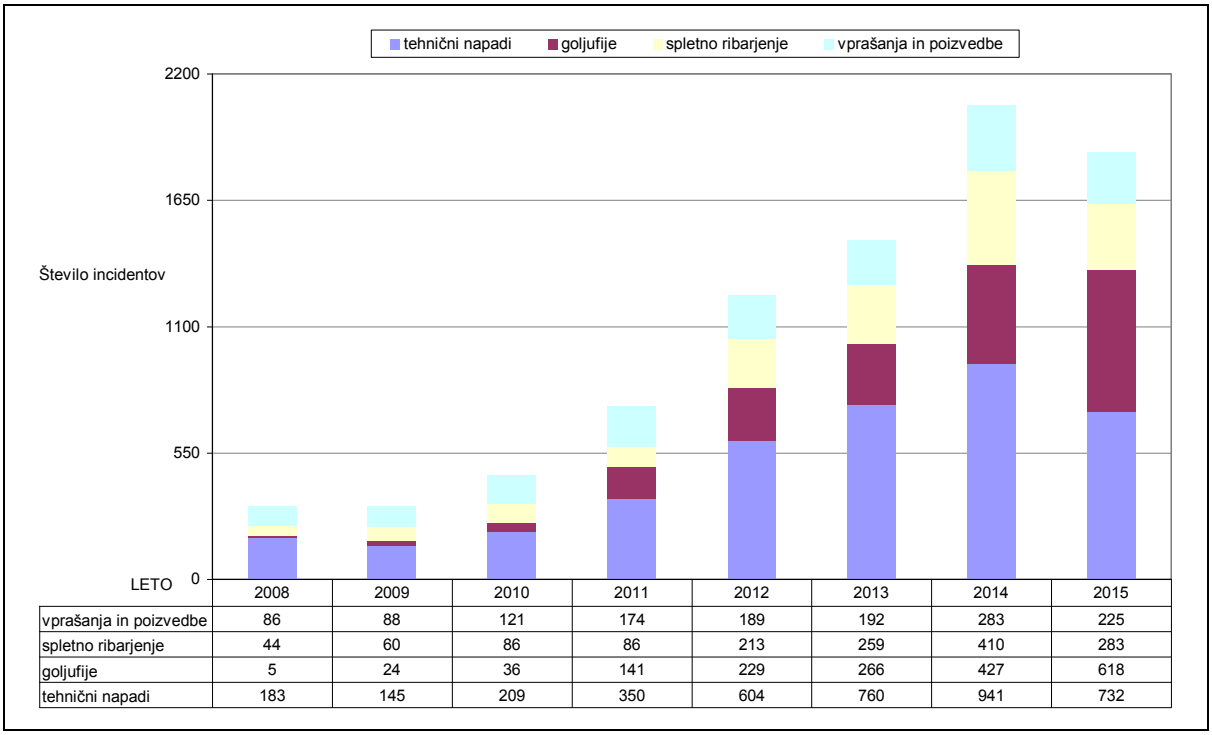
Slika 9: Graf - posledice varnostnih incidentov, s katerimi so se srečala podjetja v letu 2010, po velikosti podjetja (vir: SURS)

Da bi dobil okvirno oceno o številu incidentov ter podrobnejšo klasifikacijo, sem uporabil podatke na spletni strani SI-CERT, ki na nivoju države sprejema prijave o tovrstnih incidentih, jih beleži ter pomaga uporabnikom pri preprečevanju nadaljnje škode.

Leta 2014 je SI-CERT v Sloveniji zabeležil 2.060 incidentov, kar je šestkrat več kot leta 2008, ko jih je bilo zabeleženih le 323. V letu 2015 je trend prvič padel na 1.924 zabeleženih incidentov. Seveda je pri tem potrebno upoštevati, da gre za statistiko, kjer so upoštevane prijave podjetij in fizičnih oseb.

Na sliki 10, povzeti po poročilu SI-CERT o omrežni varnosti za leto 2015 [90], vidimo trend števila beleženih incidentov po štirih kategorijah:

- tehnični napadi (napad onemogočanja, razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij napadalca, skeniranje in poskušanje, botnet, škodljiva koda, zloraba storitve, vdor v sistem, zloraba uporabniškega računa, napad na aplikacijo);
- goljufije (lažne spletne prodajalne, prevare pri prodaji in nakupih prek spletnih posrednikov, lažni krediti, nigerijske in loterijske prevare, obljube po hitrem zaslužku);
- spletno ribarjenje ali lovljenje na limanice (kraja identitete);
- vprašanja in poizvedbe (sumljive ankete in vprašalniki z namenom zbiranja podatkov).



LETO	2008	2009	2010	2011	2012	2013	2014	2015
vprašanja in poizvedbe	86	88	121	174	189	192	283	225
spletno ribarjenje	44	60	86	86	213	259	410	283
goljufije	5	24	36	141	229	266	427	618
tehnični napadi	183	145	209	350	604	760	941	732

Slika 10: Število obravnavanih incidentov na leto, Slovenija 2008-2015 (vir: SI-CERT [85])

Za leto 2015 iz slike 10 lahko razberemo, da so se zmanjšali predvsem tehnični napadi, kjer je beležen 22% upad glede na leto 2014. Spletno ribarjenje pa beleži 20% upad glede na leto 2014. Vendar pa se je po drugi strani za 31% povečalo število goljufij. Iz tega lahko sklepamo, da se spletni kriminalci z napadov na sisteme preusmerjajo na uporabo taktik za manipulacije z ljudmi. Če se bo trend nadaljeval, lahko kmalu pričakujemo, da bo število zabeleženih goljufij preseglo število tehničnih napadov na sisteme.

4.2.2 Posledice incidentov glede na velikost podjetja, leto 2010

V tabeli 1 vidimo, da velika podjetja beležijo skoraj dvakrat večji odstotek nedosegljivosti storitev IKT, uničenja ali zlonamernega spreminjanja podatkov zaradi napake v programski ali strojni opremi kot srednje velika podjetja. Srednje velika podjetja pa imajo skoraj dvakrat toliko incidentov kot mala podjetja.

Nevarnost za nedosegljivost storitev IKT zaradi napada od zunaj (DoS) je pri velikih podjetjih skoraj dvakrat višja kot pri ostalih podjetjih.

Nevarnost za razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma je več kot trikrat višja pri velikih podjetjih glede na ostala podjetja.

V kategoriji uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa so velika podjetja na drugem mestu oziroma za srednje velikimi podjetji. Iz tega lahko sklepamo, da imajo velika podjetja v večji meri kot srednje velika podjetja urejene osnovne varnostne mehanizme, kamor spadajo antivirusni programi, protismetni e-poštni filtri (angl. antispam email filters) in urejene pravice dostopov uporabnikov (angl. identity management).

Srednje velika podjetja morajo paziti predvsem na varovanje pred uničenjem ali zlonamernim spreminjanjem podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa.

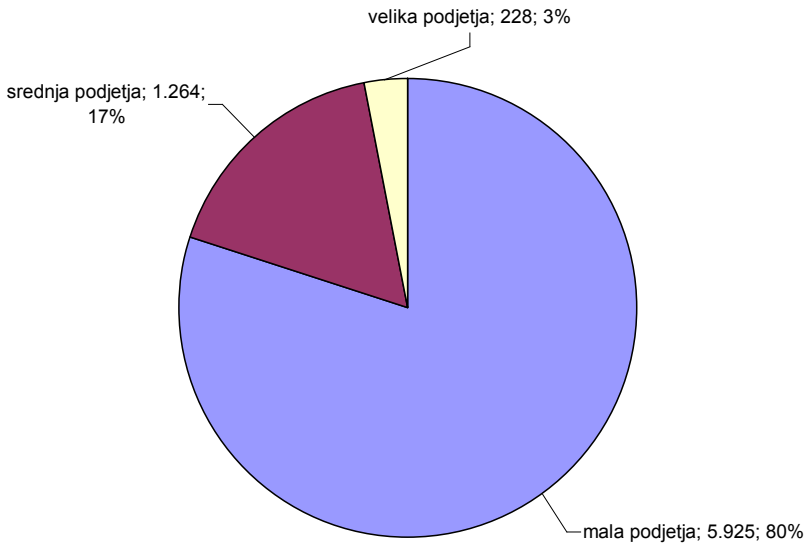
Iz zgoraj navedenega lahko sklepamo, da velika podjetja v povprečju beležijo dvakrat višji odstotek posledic varnostnih incidentov zaradi:

- napak v strojni ali programski opremi,
- napadov od zunaj (DoS),
- razkritja zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma.

Pregled teh ugotovitev potrjuje domnevo, da je ranljivost v velikih podjetjih lahko višja od ranljivosti preostalih vrstah podjetij. S tem smo pridobili dodatno osnovo za smiselnost nadaljnjih raziskav za potrjevanje hipoteze H1.

H1: Če slovensko podjetje deluje v kategoriji velikih podjetij, potem je bolj ranljivo od mikro, malih in srednje velikih slovenskih podjetij.

Potrjevanje hipoteze otežuje dejstvo, da varnostni vidiki na področju IKT vključujejo več različnih področij, in sicer nevarnost virusov, gospodarsko vohunjenje, usmerjene in naključne napade, ozaveščenost zaposlenih o varnosti IKT, uvedbo in izvajanje varnostnih standardov, namerno povzročanje škode s strani zaposlenih, odnos vodstva do organizacijske varnosti ipd. Statistični podatki pa nam kažejo le ozek segment vseh teh vidikov. Torej trije ali štirje elementi ne morejo dokazovati celotnega spektra varnosti IKT v podjetjih.



Slika 11: Delež podjetij glede na velikost podjetja (vir: SURS)

Na sliki 11 sledi še prikaz porazdelitve skupin podjetij glede na velikost podjetja v celotnem vzorcu podatkov. Vidimo, da je v vzorcu statistično obravnavanih podjetij

kar 80% malih podjetij, 17% je srednje velikih podjetij in 3% velikih podjetij z več kot 250 zaposlenimi.

4.2.3 Posledice incidentov glede na SKD podjetja

Glede na to, da obstajajo podatki o varnostnih incidentih podjetij glede na standardno klasifikacijo dejavnosti (SKD [89])[9], me je zanimalo, ali je dejavnost (sektor), v kateri deluje podjetje, povezana s številom incidentov.

V tabeli 2 so zbrane posledice varnostnih incidentov, s katerimi so se srečala podjetja v letu 2010, pri čemer so podjetja razvrščena po dejavnosti glede na SKD. Oznaka "-" pomeni "ni pojava", kar v nadaljevanju kvantitativno lahko upoštevamo kot vrednost 0. Na osnovi tabele 2 je na sliki 12 izrisan graf posledic incidentov po dejavnostih. V grafu ni izrisane kategorije TI5 (razkritje zaupnih podatkov zaradi vdora, 'pharming' ali 'phishing' napadov), ker se tovrstni incidenti pojavijo le v dejavnostih D2 in D12.

Glede na vrsto incidenta najdemo v tabeli za posamezno vrsto incidenta naslednje ugotovitve:

Nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi. V tem segmentu s 17,8% vodijo podjetja, razvrščena v D11 (55 gostinske nastanitvene dejavnosti, strežba jedi in pijač). S 3,4% imajo najmanj incidentov podjetja, ki imajo kot glavno dejavnost D12 (56 dejavnost strežbe jedi in pijač). Ta ugotovitev sloni na podatkih SURS, a je precej kontradiktorna, kajti gre za zelo sorodni dejavnosti. Pojav bi bilo smiselno bolj podrobno raziskati.

Nedosegljivost storitev IKT zaradi napada od zunaj. S 4,1% vodijo dejavnosti »69–74 strokovne, znanstvene in tehnične dejavnosti«, z 0,4% pa je na zadnjem mestu »41–43 gradbeništvo«.

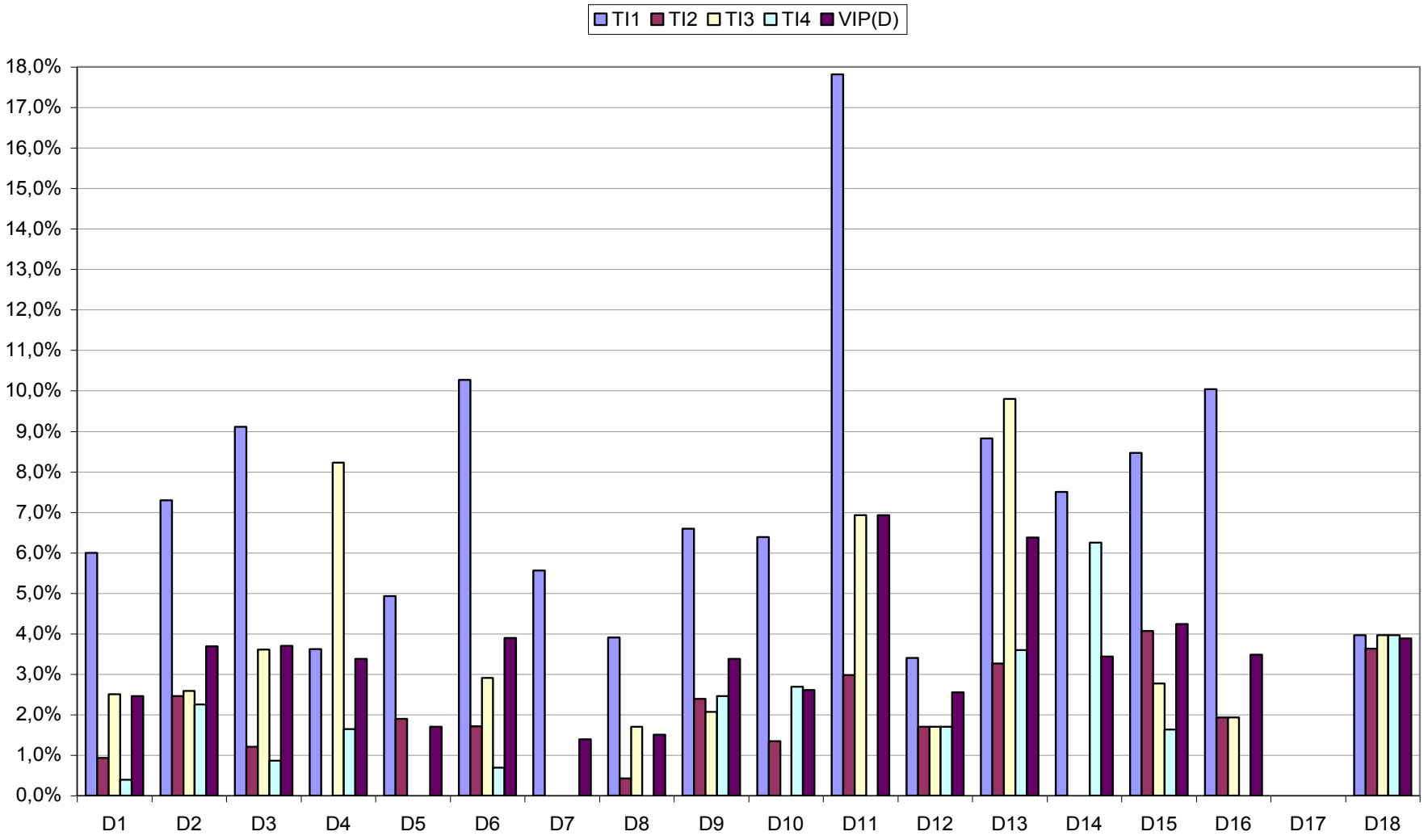
[9] http://www.ajpes.si/Registri/Drugo/SKD

Skupaj	Dejavnost (glej legendo dejavnosti)																	
povprečje	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18
TI1: Nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi																		
6,7%	6,0%	7,3%	9,1%	3,6%	4,9%	10,3%	5,6%	3,9%	6,6%	6,4%	17,8%	3,4%	8,8%	7,5%	8,5%	10,0%	-	4,0%
TI2: Nedosegljivost storitev IKT zaradi napada od zunaj																		
1,7%	0,9%	2,5%	1,2%	-	1,9%	1,7%	-	0,4%	2,4%	1,3%	3,0%	1,7%	3,3%	-	4,1%	1,9%	-	3,6%
TI3: Uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa																		
2,5%	2,5%	2,6%	3,6%	8,2%	-	2,9%	-	1,7%	2,1%	-	6,9%	1,7%	9,8%	-	2,8%	1,9%	-	4,0%
TI4: Razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma																		
1,4%	0,4%	2,3%	0,9%	1,6%	-	0,7%	-	-	2,5%	2,7%	-	1,7%	3,6%	6,3%	1,6%	-	-	4,0%
TI5: Razkritje zaupnih podatkov zaradi vdora, 'pharming' ali 'phishing' napadov																		
0,1%	-	0,2%	-	-	-	-	-	-	-	-	-	1,7%	-	-	-	-	-	-
VIP(D)[10]	2,5%	3,7%	3,7%	3,4%	1,7%	3,9%	1,4%	1,5%	3,4%	2,6%	6,9%	2,5%	6,4%	3,4%	4,2%	3,5%	-	3,9%

Tabela 2: Posledice varnostnih incidentov, s katerimi so se srečala podjetja v letu 2010, SKD (vir: SURS)

Legenda dejavnosti:
D1 Proizvodne dejavnosti (dejavnosti C–F)
D2 Storitvene dejavnosti (dejavnosti G–S)
D3 10–18 Predelovalne dejavnosti (proizvodnja živil, tekstilnih, lesnih, papirnatih izdelkov, tiskarstvo)
D4 19–23 Predelovalne dejavnosti (proizvodnja naftnih, kemičnih, farmacevtskih surovin, izdelkov iz gume, plastičnih mas, nekovinskih mineralnih izdelkov)
D5 24–25 Predelovalne dejavnosti (proizvodnja kovin, nekovin)
D6 26–33 Predelovalne dejavnosti (proizvodnja računalnikov, elektronskih izdelkov, strojev, vozil, električnih naprav)
D7 35–39 Oskrba z energijo, vodo, ravnanje z odpadki
D8 41–43 Gradbeništvo
D9 45–47 Trgovina, vzdrževanje in popravila motornih vozil
D10 49–53 Promet in skladiščenje
D11 55 Gostinske nastanitvene dejavnosti, strežba jedi in pijač
D12 56 Dejavnost strežbe jedi in pijač
D13 58–63 Informacijske in komunikacijske dejavnosti
D14 68 Poslovanje z nepremičninami
D15 69–74 Strokovne, znanstvene in tehnične dejavnosti (sem spadajo tudi Pravne dejavnosti, Pravne in računovodske dejavnosti)
D16 77–82 Druge raznovrstne poslovne dejavnosti
D17 95 Druge dejavnosti: Popravila računalnikov in izdelkov za široko rabo
D18 Sektor IKT

[10] Povprečna verjetnost (oziroma indeks), da podjetje ki deluje v določeni dejavnosti (po SKD), beleži posledice incidenta.



Slika 12: Graf varnostnih incidentov po SKD (vir: SURS)

Uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa. S 9,8% so kot najbolj izpostavljene dejavnosti »58–63 informacijske in komunikacijske dejavnosti«, z 1,7% pa je najmanj izpostavljena dejavnost »41-43 gradbeništvo«.

Razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma. S 6,3% je na prvem mestu dejavnost »68 poslovanje z nepremičninami« in z 0,4% so kot najmanj izpostavljene dejavnosti »proizvodne dejavnosti (dejavnosti C–F)«.

Razkritje zaupnih podatkov zaradi vdora, 'pharming' ali 'phishing' napadov so zabeležila le podjetja v D2 (storitvene dejavnosti (dejavnosti G–S)) v 0,2% ter podjetja v D12 (56 dejavnost strežbe jedi in pijač) z 1,7%. Ostala podjetja posledic teh incidentov niso beležila.

Vrednost **VIP(D)** v zadnji vrstici tabele 2 in na sliki 9 pomeni povprečno verjetnost (oziroma indeks), da v podjetju, ki se ukvarja z določeno dejavnostjo, pride do incidenta. Predpostavil sem, da se incident odrazi v vseh štirih kategorijah incidentov, ki so navedeni v poglavju **Error! Reference source not found.**, zato sem za določeno dejavnost seštel vse incidente in vsoto delil s štiri (toliko je namreč kategorij incidentov) in potem še s številom podjetij (4.1). Vsoto incidentov v posamezni dejavnosti sem delil s številom kategorij incidentov zato, ker v enem podjetju lahko pride tudi do incidentov, ki se odrazijo v vseh štirih (neodvisnih) kategorijah. Zato je potrebno vrednost normalizirati.

$$VIP(D) = \frac{1}{4}\sum_{j=}^{\cdot} \; r_j \cdot \frac{1}{stPodjetij\,(D)} \qquad (4.1)$$

Po stopnji verjetnosti incidenta v podjetju glede na dejavnost s 6,5% vodijo dejavnosti D18 (64.19, 64.92 drugo denarno posredništvo, drugo kreditiranje), s 6,4% pa jim tesno sledijo dejavnosti »58–63 informacijske in komunikacijske dejavnosti«, z 1,4% incidentov pa je na zadnjem mestu kot najbolj varna dejavnost »35–39 oskrba z energijo, vodo, ravnanje z odpadki«, ki ji z 1,5% tesno sledi dejavnost »41-43 gradbeništvo«. Dejavnost D17 (95 druge dejavnosti: popravila računalnikov in izdelkov za široko rabo) ima pri vseh kategorijah posledic incidentov oznako "-", kar pomeni "ni pojava". Teoretično to pomeni, da je D17 najvarnejša dejavnost, vendar se pojavlja dvom o točnosti teh statističnih podatkov.

Lahko bi sicer sklepali, da manj kot ima podjetje IKT opreme, manj je ranljivo za grožnje na področju IKT, vendar ne poznamo vseh ostalih dejavnikov, ki vplivajo na varnost IKT. Lahko bi namreč napačno sklepali, da ima neko podjetje malo IKT opreme, glede na to, da tega iz statističnih podatkov ne moremo razbrati. Po drugi strani obstaja tudi možnost, da zaposleni v podjetju zaradi pomanjkljivega znanja ne zaznajo varnostnih incidentov ali pa incidente zaznajo, a ker jih iz različnih vzrokov (skrb za delovno mesto, malomarnost, skrb za svoj strokovni ugled, ego ipd.) ne uspejo dovolj učinkovito preprečiti, enostavno o njih ne poročajo naprej.

4.2.4 Analiza porazdelitve števila incidentov po SKD

Porazdelitev števila posledic incidentov po SKD podjetij je zbrana v tabeli 3.

	Dejavnost (glej legendo v tabeli 2)																	
	D1	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**	**D9**	**D10**	**D11**	**D12**	**D13**	**D14**	**D15**	**D16**	**D17**	**D18**
TI1	213	282	53	11	26	60	8	55	102	38	18	12	27	6	52	26	0	12
TI2	33	95	7	0	10	10	0	6	37	8	3	6	10	0	25	5	0	11
TI3	89	100	21	25	0	17	0	24	32	0	7	6	30	0	17	5	0	12
TI4	14	87	5	5	0	4	0	0	38	16	0	6	11	5	10	0	0	12
TI5	0	6	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0

Tabela 3: Število incidentov po SKD. Upoštevana so le podjetja, ki so beležila posledice TI (vir: SURS)

Na osnovi podatkov v tabeli 3 in grafa na sliki 12 lahko podam naslednji odgovor na raziskovalno vprašanje RV2:

Porazdelitev posledic incidentov slovenskih podjetij kaže na to, da je število posledic varnostnih incidentov različno glede na vrsto dejavnosti (po SKD), v kateri podjetja delujejo. To odpira osnovo za nadaljnje raziskave, brez katerih ne moremo sklepati, da so podjetja v določeni dejavnosti bolj ranljiva. Prav tako brez nadaljnjih raziskav ne moremo ugotoviti, kolikšen vpliv ima dejavnost na število posledic incidentov.

Na število incidentov namreč, kot je bilo že večkrat poudarjeno, vpliva mnogo dejavnikov, med katerimi so tudi:

- izpostavljenost določene dejavnosti (po SKD) zunanjim in notranjim grožnjam;
- dejanska tehnična ranljivost sistemov IKT v organizaciji;
- ozaveščenost zaposlenih;
- organizacijska kultura;
- odnos vodstva do varnosti ipd.

4.2.5 Podjetja v finančnem sektorju

Podjetja, ki delujejo v finančnem sektorju, so bila v statističnih analizah obravnavana ločeno. To je razumljivo, saj se ukvarjajo s finančnimi transakcijami organizacij in posameznikov, ki so povezane z občutljivimi informacijami in so vezane na osebne oziroma zaupne podatke. Nekatere statistike niso bile na voljo in so v tabeli označene z "z" - oznaka zaupno ali "-" - ni podatkov. Kljub temu je bilo na voljo dovolj podatkov za izračun povprečja posledic TI1 za vsa podjetja v finančnem sektorju in tista podjetja z 250 ali več zaposlenimi.

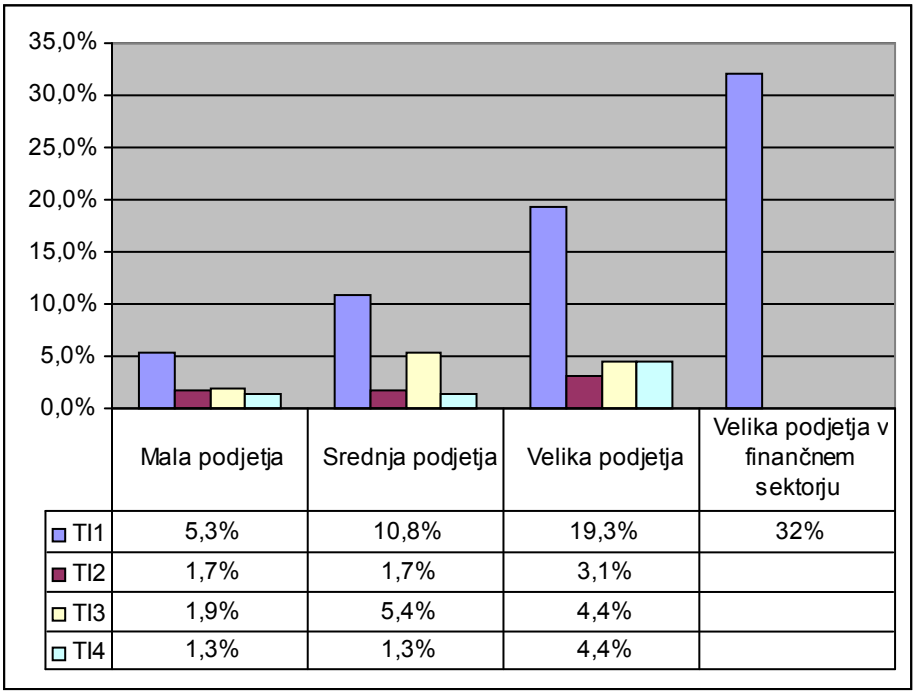
Obravnavana podjetja delujejo v naslednjih dejavnostih:

a) 64.19, 64.92 drugo denarno posredništvo, drugo kreditiranje;
b) 65.1, 65.2 dejavnost zavarovanja, pozavarovanja;
c) 66.12, 66.19 posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade.

Tip incidenta	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
TI1: Nedosegljivost storitev IKT uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi	19%[11]	z	z	32%

Tabela 4: Posledice varnostnih incidentov, s katerimi so se srečala podjetja v finančnem sektorju v letu 2010, po številu zaposlenih (vir: SURS)

V tabeli 4 vidimo, da v finančnem sektorju v povprečju 19 podjetij beleži incidente na področju »nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi«. To je kar za 12% več kot ostala podjetja. Števila ostalih tipov ranljivosti statistični podatki SURS ne razkrivajo.



	Mala podjetja	Srednja podjetja	Velika podjetja	Velika podjetja v finančnem sektorju
TI1	5,3%	10,8%	19,3%	32%
TI2	1,7%	1,7%	3,1%	
TI3	1,9%	5,4%	4,4%	
TI4	1,3%	1,3%	4,4%	

Slika 13: Tabela in graf posledic TI – primerjava med podjetji po velikosti, dodatno velika podjetja v finančnem sektorju (vir: SURS)

Nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi v letu 2010 beležijo pri kar 32% velikih podjetij v finančnem sektorju, kar je za 13% več kot pri ostalih velikih podjetjih. Nazoren prikaz na sliki 13. Prazne podatkovne celice za podjetja v finančnem sektorju pomenijo, da teh podatkov ni bilo na voljo, zato je tudi graf izrisan le za TI1.

Če primerjamo povprečno vrednost TI1 za podjetja v finančnem sektorju (19%) z ostalimi vrstami podjetij po SKD (tabela 2), vidimo, da finančni sektor beleži najvišji procent posledic IK1. Za finančnim sektorjem so s 17,8% gostinske nastanitvene dejavnosti, strežba jedi in pijač (D11).

[11] Izračunano na osnovi dostopnih podatkov SURS. Kljub temu da SURS nekaterih podatkov ne navaja (oznaka zaupno), pa so dostopni podatki o številu vseh podjetij v vzorcu in številu vseh podjetij z več kot 10 zaposlenimi, ki so beležila TI1.

Če pa primerjamo podjetja v finančnem sektorju in posledice TI1 z vsemi ostalimi vrstami podjetij zgolj po velikosti podjetja (tabela 1), vidimo, da finančni sektor z 19% beleži v povprečju približno 2,7-krat višji procent posledic TI1 od povprečja ostalih podjetij (7%).

Pri tem se moramo zavedati, da je pri določenih podjetjih, predvsem tistih, ki delujejo na področju finančnih storitev, motiv zlonamernežev ali organizacij, da izkoristijo ranljivost teh podjetij, večji. Iz tega razloga lahko pri isti stopnji ranljivosti zaradi večjega obsega groženj pride do večjega števila incidentov. Upoštevati pa je potrebno tudi to, da imajo podjetja v finančnem sektorju zaradi narave poslovanja več kontrol nad svojimi sistemi IKT in verjetno zaznajo večje število dejanskih incidentov kot podjetja, kjer poslovanje ni tako kritično z vidika varnosti in neprekinjenega poslovanja.

4.2.6 Ugotovitve in priporočila za slovensko gospodarstvo

Glede na odstotek incidentov po velikosti podjetij in po dejavnosti ter na podlagi razpoložljivih podatkov lahko predvidevamo, da so **v Sloveniji najbolj ranljiva velika podjetja v finančnem sektorju.**

Glede na ostale statistične analize bom v nadaljevanju poskušal najti še dodatne potrditve za zgornjo trditev. Precej verjetno pa drži, da so zaradi velikosti in prepoznavnosti takšna podjetja veliko pogosteje tarča napadalcev, saj se ti zavedajo, da z uspešno izvedenim incidentom pridobijo veliko večje koristi (finančne informacije/transakcije, osebne podatke, ipd.) kot pri majhnih podjetjih.

V stolpcu D15 (69–74 strokovne, znanstvene in tehnične dejavnosti; sem spadajo tudi pravne dejavnosti ter pravne in računovodske dejavnosti) v tabeli 2 vidimo, da so bile te dejavnosti že v letu 2010 pogosto tarča zunanjih napadov na njihove sisteme IKT. Današnje svetovne statistike kažejo trend rasti incidentov v tem sektorju, zato je priporočljivo, da podjetja v navedenih dejavnostih namenijo potreben poudarek izboljšanju varnosti svojih sistemov IKT in izobraževanju zaposlenih na področju organizacijske varnosti.

4.2.7 Priporočila za podjetja v finančnem sektorju

Predlagam naslednje smernice, ki so bile v [3] zapisane kot lekcije, ki se jih je naučila francoska banka Société Générale potem, ko so v letu 2008 ugotovili izgubo sedem milijard USD. To se je zgodilo zaradi notranje zlorabe in neavtoriziranih transakcij zaposlenega borznega trgovca Jeroma Kerviel-a. Vodstvo je občasno opazilo anomalije pri dostopu do sistemov izven delovnega časa in pri trgovalnih transakcijah, vendar je Jerome vedno uspel biti korak pred vodstvom (notranjo kontrolo) in je zakril ali racionalno razložil svoje delovanje. Te lekcije so uporabne zlasti za podjetja v finančnem sektorju in tudi za ostale organizacije.

1. Zaznava in merjenje pravih tveganj

Ključna težava v Société Générale je bila, da so upravljali le tveganja na trgu, ne pa tudi operativnih notranjih tveganj, kjer lahko pride do goljufij zaposlenih pri

nepooblaščenih transakcijah. Podoben primer za podjetje, ki ima spletno trgovino, bi bil, da upravlja le s tveganji na trgu in s tehničnimi tveganji pri delovanju spletne trgovine, medtem ko zaposleni uporabljajo na papir natisnjene sezname številk kreditnih kartic kupcev. Poleg tega se takšni seznami ne uničijo v skladu z varnostnimi postopki, temveč končajo v smetnjaku za papir.

2. Varovanje in upravljanje gesel
Ena večjih težav je, da zaposleni pogosto slabo varujejo svoja uporabniška gesla. Gesla je moč enostavno uganiti, ker so preenostavna ali pa jih imajo zaposleni celo zapisana nekje blizu računalnika. Da bi zmanjšali tveganja za "izgubo" gesel, je potrebno zaposlene izobraziti o pomembnosti skrbnega ravnanja z gesli. Uporabljajo naj kompleksna gesla, pogosto naj jih menjajo in jih ne zaupajo nikomur. Zavedati se morajo, da lahko z njihovim geslom napadalec (notranji ali zunanji) zlorabi njihove dostopne pravice za povzročanje nadaljnje škode ali krajo podatkov. V pomoč pri zmanjšanju napadov na gesla so tudi enkratna gesla in strojni žetoni (fizični čip ali kartica), ki so v kombinaciji s pravim geslom potrebni za avtentikacijo v sistemu.

3. Nadzor dnevniških datotek
Današnji sistemi beležijo veliko število legitimnih akcij in tudi akcij, ki so sprožile napako ali zavrnitev dostopa. Seveda pa ti zapisi nimajo pomena, če jih ne pregledujemo in preverjamo.

Primer takšnega preverjanja:
Zakaj je nekdo pogosto prijavljen v sistemu izven delovnega časa?
Zakaj je oseba X v času Y vstopila in izstopila iz varovanega področja (na primer strežniška varovana soba)?

Priporočljivo je, da takšne dogodke beležimo tam, kjer se zgodijo (delovna postaja, strežniška soba, spletni strežnik ipd.) in jih spremljamo preko centralnega sistema za nadzor in evalvacijo dnevniških dogodkov. Najbolje je nastaviti sistem tako, da pri določenih prednastavljenih pravilih sproži alarm (obvestilo na email, telefon ipd), da odgovorni lahko takoj preverijo stanje sistemov in osebja (če gre za človeški faktor) ter primerno ukrepajo.

4. Pravilna zasnova varnostnih sistemov
Ne smemo se zanašati na to, da napadalec ne ve, kako je zastavljen varnostni sistem, kajti lahko pride do notranje zlorabe, kjer bo nekdo, ki ima znanje o sistemu, z lahkoto obšel varnostne mehanizme.

Varnostni sistemi tako tehnični kot tisti, ki vključujejo ljudi, kot so na primer nadzorniki, varnostna služba ipd., morajo biti zasnovani tako, da ima napadalec lahko vse informacije o delovanju varnostnega sistema, vendar ga kljub temu ne more obiti.

5. Celovito varovanje sredstev organizacije
Pogosto se organizacije osredotočajo le na zunanje grožnje: napadi na spletne strežnike preko interneta, prispela zlonamerna pošta v elektronski pošti zaposlenih, fizično varovanje vstopa neznancem v prostore organizacije ipd.

Obenem pa pozabljajo, da se lahko zloraba ali prekoračitev pooblastil zgodi tudi s strani zaposlene osebe. Prav zato morajo biti varnostne politike postavljene na način, da prvenstveno varujejo sredstva organizacije in ne služijo zgolj zaščiti pred zunanjimi grožnjami. S tem bo tveganje za zunanjo ali notranjo zlorabo ali za ogrožanje sredstev organizacije manjše.

6. Upravljanje z identitetami (pravicami in vlogami) zaposlenih
Ko oseba zapusti organizacijo, je potrebno ukiniti njene pristopne pravice ali vsaj zamenjati geslo, če bi popolna ukinitev uporabniškega pristopa vplivala na dostop do podatkov, ki jih organizacija potrebuje za nadaljnje poslovanje.

Prav tako je potrebno v zvezi z uporabniškim dostopom do IKT sistemov osebi, ki menja delovno mesto oziroma funkcijo znotraj organizacije, pravilno dodeliti nove pravice in umakniti stare pravice. Če se stare pravice ne ukinejo, se lahko zgodi, da bo oseba zaradi menjave delovnih mest znotraj organizacije na koncu imela nakopičene (agregirane) pravice vseh delovnih mest oziroma funkcij, na katerih je opravljala delo. To pa pomeni tudi možno zlorabo. Prav to je omogočilo zgoraj omenjenemu Kervielu, da je lahko sam potrjeval transakcije, ki bi jih sicer moral potrditi njegov nadrejeni na novem delovnem mestu.

7. Družbeni inženiring je grožnja, ki se je premalo zavedamo
Ljudje smo v svoji naravi zaupljivi do bližnjih in radi verjamemo njihovi razlagi nastalih dejstev. Vendar pa se je potrebno zavedati, da je to zaupanje lahko podlaga za to, da notranja oseba v organizaciji s pretvezo pridobi geslo svojega sodelavca in zlorabi njegov dostop. Najbolje se je držati pravila: "Zaupaj, vendar vedno preveri."

8. Previdnost pri delu s prejetimi sporočili e-pošte
Lahko bi rekli, da je to nadaljevanje prejšnje točke. Zaposlene je potrebno izobraziti, da ne zaupajo slepo prejetemu sporočilu e-pošte, četudi je v polju "od" (angl. from) naziv njihovega nadrejenega. Potrebno se je zavedati, da je dokaj enostavno mogoče potvoriti glavo email sporočila in s tem tudi vir pošiljatelja, kljub temu da je vsebina email sporočila digitalno podpisana. Zaradi tehničnih omejitev v nekaterih primerih namreč tehnologiji za varen prenos email sporočil (S/MIME ali PGP) ne podpišeta glave sporočila, temveč samo vsebino sporočila. To pa omogoča spremembo glave sporočila, ne da bi to vplivalo na avtentičnost vsebine sporočila.

V primeru kakršnegakoli suma pri prejemu takšnega sporočila naj prejemnik preveri avtentičnost sporočila pri domnevnem pošiljatelju preko drugega komunikacijskega kanala. Lahko ga na primer pokliče po telefonu in povpraša glede sporočila ali pa se sprehodi do njegove pisarne in osebno preveri, ali je v sporočilu navedeni pošiljatelj resnično poslal omenjeno sporočilo.

9. Previdno pri zmanjševanju zaposlenih
Organizacije so v času krize med letoma 2008 in 2012 pogosto zmanjševale kadre v oddelkih, ki so bili na seznamu stroškovnih in neprofitnih centrov. Na tem seznamu se je znašel tudi IT oddelek, znotraj njega pa osebje, ki ni bilo nujno potrebno za nemoteno poslovanje. Vendar pa se odpuščanje kadra na področju

upravljanja s tveganji številnim organizacijam ni izplačalo, saj so v primeru napada utrpele škodo, ki je vsaj nekajkrat presegala strošek plač osebja za varnost in upravljanje s tveganji.

10. Preverjanje, preverjanje, preverjanje

Ali sistemi (tehnični in tisti, ki so odvisni od človeškega dejavnika) pravilno delujejo in zagotavljajo potrebne dnevniške zapise, preko katerih je moč slediti akcijam in zaznati odstopanja od normalnega delovanja? Dostikrat se v praksi zgodi, da je zasnova in postavitev sistemov dobro načrtovana in izvedena, vendar pa ne deluje z vsemi zasnovanimi varnostnimi kontrolami in postopki. Razlogov za to je več in pogosto je tudi poslovodstvo organizacije seznanjeno s tem. Tako je bilo tudi v primeru Société Générale, saj je prav uprava dovolila izklop kontrole določenim borznim trgovcem, ker so te kontrole upočasnjevale transakcije.

V praksi se takšne stvari pogosto dogajajo z vedenjem vodstva. Podoben je primer slovenskega podjetja izpred nekaj let, ko poslovodstvo dolgo časa ni bilo pripravljeno odobriti nakupa novih strežnikov, IT oddelek pa je bil zaradi zahtev po hitrosti delovanja sistemov prisiljen izklopiti vse nepotrebne kontrole in funkcije. Med drugim so izklopili tudi zapis dnevniških datotek na spletnih strežnikih, varnostne kopije pa so se namesto vsak dan vršile le še med vikendi. Zaradi preobremenjenosti so odpovedovali diski v strežnikih in za skoraj vsakodnevno urgentno reševanje je bilo porabljenih toliko delovnih človek/ur, da bi s tem denarjem lahko kupili dvakrat zmogljivejše strežnike, ki so jih sicer na koncu le kupili.

Organizacije naj torej periodično preverjajo, ali varnostne kontrole in postopki v praksi delujejo, kot je bilo načrtovano. Kot smo zapisali v poglavju o standardih, leti to predvidevajo, zato je za organizacije najbolje, da sledijo zahtevam in priporočilom standarda ISO/IEC 27001 oziroma sorodnim standardom.

4.3 Formalne strategije za varno uporabo IKT z načrtom za njen redni pregled

4.3.1 Statistični podatki za slovenska podjetja v letu 2010

Razlaga novih pojmov v tem poglavju

Podjetje je imelo formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled: Pod varnost pri uporabi IKT štejemo ukrepe, nadzor in postopke za zagotavljanje integritete, verodostojnosti, dostopnosti in zaupnosti podatkov in sistemov IKT.

Nepredviden dogodek: napaka na strojni ali programski opremi, nepooblaščen dostop.

Med podjetji z vsaj 10 zaposlenimi je v januarju 2010 imelo formalno določeno strategijo za varno uporabo IKT 16% podjetij (tabela 5), navaja SURS. Tovrstna strategija vsebuje predvidene ukrepe, nadzor in postopke za zagotavljanje dostopnosti, verodostojnosti in zaupnosti podatkov ter sistemov IKT.

Med podjetji v storitvenih dejavnostih je bilo takšnih podjetij 21%, med podjetji v proizvodnih dejavnostih pa 11%. Na prvih dveh mestih so s 50% informacijske in komunikacijske dejavnosti ter druge dejavnosti (popravila računalnikov in izdelkov za široko rabo), s 45% pa sledi sektor IKT. Na zadnjem mestu je gradbeništvo z le 6% formalno določenih strategij za varno uporabo IKT (tabela 6).

Med podjetji z omenjeno strategijo v letu 2010 jih je imelo 91% v le-to vključeno tudi nevarnost uničenja ali zlonamernega spreminjanja podatkov zaradi napada ali nepredvidenega dogodka. 77% podjetij je zajelo nevarnost razkritja zaupnih podatkov kot posledico vdora ali napada »pharming« oz. »phishing«, 75% podjetij pa neuporabnost storitev IKT zaradi napada od zunaj, tipa DDoS (zavrnitev storitve).

V tabeli 5 je narejena primerjava urejenosti formalnih strategij za varno uporabo IKT po velikosti podjetij za leto 2010 in 2015.

Ugotavljam, da je v petih letih (od 2010 do 2015) najbolj napredovala urejenost formalnih strategij pri malih podjetjih (10-49 zaposlenih). Napredek je bil v povprečju za 4% letno. Ostale vrednosti so v prid vzpostavitve formalnih strategij pridobivale med 2% in 4% letno.

Sledila so srednja podjetja s povprečnim faktorjem 2.0 (podvojitev postavljenih formalnih strategij v petih letih). Na zadnjem mestu so velika podjetja s faktorjem 1.4. Tu je potrebno omeniti, da je že v letu 2010 imelo urejene formalne strategije 46% velikih podjetij, v letu 2015 pa kar 66%.

	Leto 2010				Leto 2015			
	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
S1: Podjetje imelo formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled	16%	12%	30%	46%	35%	30%	53%	66%
S2: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov zaradi napada ali nepredvidenega dogodka	15%	11%	27%	43%	32%	28%	47%	62%
S3: Strategija zajemala nevarnost razkritja zaupnih podatkov zaradi vdora, 'pharming', 'phishing' napadov ali nehote	12%	10%	21%	36%	28%	25%	41%	51%
S4: Strategija zajemala nevarnost neuporabnosti storitev zaradi napada od zunaj (DDoS)	12%	10%	20%	34%	26%	22%	41%	43%
S5: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov, razkritje zaupnih podatkov in neuporabnost storitev IKT zaradi napada od zunaj	11%	9%	17%	32%	23%	20%	37%	41%
S6: Strategija določena ali zadnjič pregledana – v zadnjih 12 mesecih	-	-	-	-	27%	24%	40%	46%
S7: Strategija določena ali zadnjič pregledana – pred več kot 12 meseci in manj kot 24 meseci	-	-	-	-	5%	4%	10%	12%
S8: Strategija določena ali zadnjič pregledana – pred več kot 24 meseci	-	-	-	-	3%	2%	3%	8%
S9: Strategija določena ali zadnjič pregledana – v zadnjih 24 mesecih	-	-	-	-	32%	28%	50%	58%

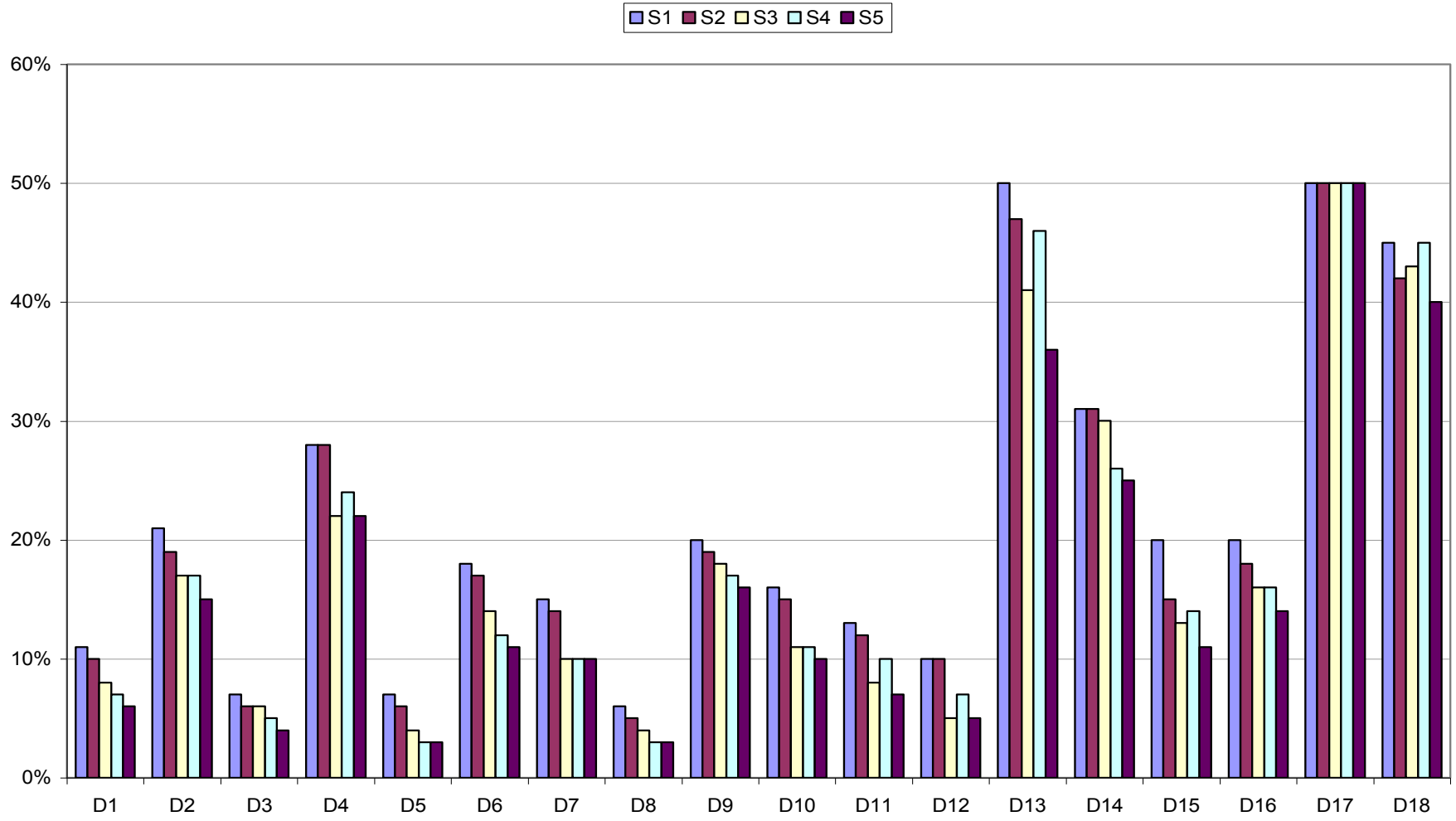
Tabela 5: Formalne strategije za varno uporabo IKT z načrtom za njen redni pregled, leto 2010, 2015 (vir: SURS)

Legenda SKD →	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18
S1: Podjetja imela formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled	11%	21%	7%	28%	7%	18%	15%	6%	20%	16%	13%	10%	50%	31%	20%	20%	50%	45%
S2: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov zaradi napada ali nepredvidenega dogodka	10%	19%	6%	28%	6%	17%	14%	5%	19%	15%	12%	10%	47%	31%	15%	18%	50%	42%
S3: Strategija zajemala nevarnost razkritja zaupnih podatkov zaradi vdora, 'pharming', 'phishing' napadov ali nehote	8%	17%	6%	22%	4%	14%	10%	4%	18%	11%	8%	5%	41%	30%	13%	16%	50%	43%
S4: Strategija zajemala nevarnost neuporabnosti storitev zaradi napada od zunaj (DDoS)	7%	17%	5%	24%	3%	12%	10%	3%	17%	11%	10%	7%	46%	26%	14%	16%	50%	45%
S5: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov, razkritje zaupnih podatkov in neuporabnost storitev IKT zaradi napada od zunaj	6%	15%	4%	22%	3%	11%	10%	3%	16%	10%	7%	5%	36%	25%	11%	14%	50%	40%

Tabela 6: Formalne strategije za varno uporabo IKT z načrtom za njen redni pregled po SKD, leto 2010 (vir: SURS)

Legenda dejavnosti:

D1 Proizvodne dejavnosti (dejavnosti C–F)
D2 Storitvene dejavnosti (dejavnosti G–S)
D3 10–18 Predelovalne dejavnosti (proizvodnja živil, tekstilnih, lesnih, papirnatih izdelkov, tiskarstvo)
D4 19–23 Predelovalne dejavnosti (proizvodnja naftnih, kemičnih, farmacevtskih surovin, izdelkov iz gume, plastičnih mas, nekovinskih mineralnih izdelkov)
D5 24–25 Predelovalne dejavnosti (proizvodnja kovin, nekovin)
D6 26–33 Predelovalne dejavnosti (proizvodnja računalnikov, elektronskih izdelkov, strojev, vozil, električnih naprav)
D7 35–39 Oskrba z energijo, vodo, ravnanje z odpadki
D8 41–43 Gradbeništvo
D9 45–47 Trgovina, vzdrževanje in popravila motornih vozil
D10 49–53 Promet in skladiščenje
D11 55 Gostinske nastanitvene dejavnosti, strežba jedi in pijač
D12 56 Dejavnost strežbe jedi in pijač
D13 58–63 Informacijske in komunikacijske dejavnosti
D14 68 Poslovanje z nepremičninami
D15 69–74 Strokovne, znanstvene in tehnične dejavnosti (sem spadajo tudi Pravne dejavnosti, Pravne in računovodske dejavnosti)
D16 77–82 Druge raznovrstne poslovne dejavnosti
D17 95 Druge dejavnosti: Popravila računalnikov in izdelkov za široko rabo
D18 Sektor IKT



Slika 14: Formalne strategije za varno uporabo IKT z načrtom za njen redni pregled po SKD, leto 2010 (vir: SURS)

4.3.2 Formalne strategije za varno uporabo IKT v finančnem sektorju

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
S1: Podjetja imela formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled	73%	56%	z	z
S2: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov zaradi napada ali nepredvidenega dogodka	68%	z	z	z
S3: Strategija zajemala nevarnost razkritja zaupnih podatkov zaradi vdora, 'pharming', 'phishing' napadov ali nehote	59%	36%	87%	68%
S4: Strategija zajemala nevarnost neuporabnosti storitev zaradi napada od zunaj (DDoS)	56%	32%	80%	68%
S5: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov, razkritje zaupnih podatkov in neuporabnost storitev IKT zaradi napada od zunaj	53%	28%	73%	68%

Tabela 7: Formalne strategije za varno uporabo IKT z načrtom za njen redni pregled v podjetjih po velikosti v finančnem sektorju 2010 (vir: SURS)

	64.19, 64.92 Drugo denarno posredništvo, drugo kreditiranje	65.1, 65.2 Dejavnost zavarovanja, pozavarovanja	66.12, 66.19 Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade
S1: Podjetja imela formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled	85%	63%	62%
S2: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov zaradi napada ali nepredvidenega dogodka	85%	z	z
S3: Strategija zajemala nevarnost razkritja zaupnih podatkov zaradi vdora, 'pharming', 'phishing' napadov ali nehote	z	37%	z
S4: Strategija zajemala nevarnost neuporabnosti storitev zaradi napada od zunaj (DDoS)	z	37%	z
S5: Strategija zajemala nevarnost uničenja ali zlonamernega spreminjanja podatkov, razkritje zaupnih podatkov in neuporabnost storitev IKT zaradi napada od zunaj	78%	32%	31%

Tabela 8: Formalne strategije za varno uporabo IKT z načrtom za njen redni pregled v podjetjih glede na SKD v finančnem sektorju v 2010 (vir: SURS)

V tabeli 7 so zbrani statistični podatki za finančni sektor (oznaka "z" v tabelah pomeni zaupno in teh podatkov ni bilo moč pridobiti). Za velika podjetja v finančnem sektorju v primerjavi s srednje velikimi podjetji je (glede na znane in manjkajoče podatke) mogoče sklepati, da je imelo v razredu velikih podjetij manj podjetij vzpostavljeno formalno IKT strategijo kot v razredu srednjih podjetij. Glede na ugotovitve v razdelku 4.2.6, da so prav velika podjetja beležila največ incidentov, menim, da je nujno, da sistematično vzpostavijo varnostne politike.

Primerjava podjetij v ostalih SKD s podjetji, ki delujejo v finančnem sektorju (tabeli 5 in 7) kaže, da tako po številu incidentov kot tudi po številu vpeljanih formalnih strategij za varno uporabo IKT prednjačijo velika podjetja z 250 ali več zaposlenimi. Izjema so le srednje velika podjetja v finančnem sektorju, ki imajo to področje bolje urejeno kot velika podjetja v finančnem sektorju. Koristno bi bilo, če bi imeli na voljo še informacijo, ali so imela podjetja, ki so utrpela posledice varnostnih incidentov, sprejete formalne strategije za varno uporabo IKT. Vsekakor pa lahko sklepamo, da imajo velika podjetja v povprečju IKT področje formalno bolje urejeno kot mikro, mala in srednja podjetja.

Tabela 8 sporoča še to, da je najmanj formalnih strategij uvedenih prav v dejavnostih »66.12, 66.19 posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade«.

4.3.3 Ugotovitve in priporočila za slovensko gospodarstvo

Priporočilo: Predvsem velika podjetja na področju »Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade« naj vzpostavijo kakovostne formalne strategije za varno uporabo IKT.

Primerjava števila formalno sprejetih strategij za varno uporabo IKT in števila posledic incidentov v 2010 po podjetjih ter nevarnosti, ki so bile zajete v teh varnostnih politikah, pokaže, da te strategije ne zmanjšajo števila incidentov. Žal te primerjave zaradi pomanjkljivih ali zaupnih podatkov ne moremo preveriti tudi za podjetja, ki delujejo v finančnem sektorju. Iz tega lahko sklepamo naslednje:

1) Število sistemov IKT: Večje kot je podjetje, več IKT uporablja, zaradi česar je bolj izpostavljeno tovrstnim ranljivostim.
2) Grožnje: Večje kot je podjetje, bolj je zanimivo za potencialne zlonamerneže. Statistično gledano so velika podjetja bolj zanimiva za napade (notranje, zunanje). Razpolagajo namreč z večjo količino podatkov in verjetno tudi z več intelektualne lastnine ter ostalih informacij (dobavitelji, kupci, finančne transakcije) in so tako zanimivejša za potencialnega napadalca.
3) Formalizacija: Velike organizacije že po svoji naravi težijo k formalizaciji postopkov, saj je to nujno, da z rastjo ostanejo obvladljive. S pravilnim pristopom pri formalizaciji IKT opreme se lahko močno zmanjša tudi ranljivost organizacije na tem področju.

4) Zunanje okoliščine: ugled, zaupanje strank in partnerjev, vrednost podatkov, število napadov, število dejanskih incidentov, zahteve partnerjev za skladnost s standardi in podobno, silijo podjetja k urejanju formalnih IKT strategij.
5) Večje kot je podjetje, bolj se zaveda in meri aktivnosti uporabnikov (glej tabelo 13) ter tudi v večji meri uporablja namenski varnostni sistem za ugotavljanje varnostnih incidentov (47% velikih podjetij).
6) Iz prejšnje ugotovitve bi lahko tudi sklepali, da je dejansko med malimi in srednje velikimi podjetji več incidentov kot kažejo statistični podatki, vendar ti incidetni sploh niso bili zaznani. To pomeni, da se ta podjetja morda niti ne zavedajo, da je prišlo do incidenta.

4.4 Seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih

4.4.1 Pregled statističnih podatkov glede na velikost podjetja

V letu 2010 je v povprečju 62% podjetij imelo opredeljen način seznanjanja zaposlenih z njihovimi obveznostmi glede varne uporabe IKT, 21% od anketiranih podjetij jih je to izvedlo z obveznim izobraževanjem, 31% ob podpisu pogodbe (o zaposlitvi) ter 51% s prostovoljnim izobraževanjem ali s splošno dosegljivimi informacijami (tabela 9).

Pri tem so dosegla najvišji odstotek velika podjetja, ki so seznanila uslužbence z njihovimi obveznostmi glede varne uporabe IKT v 91% , pri čemer so to storila z obveznim izobraževanjem ali predstavitvami v 40%.

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
Podjetja seznanila uslužbence z njihovimi obveznostmi glede varne uporabe IKT	62%	57%	79%	95%
...z obveznim izobraževanjem ali predstavitvami	21%	18%	31%	40%
..pri podpisu pogodbe, npr. pogodbe o zaposlitvi	31%	26%	45%	60%
..s prostovoljnim izobraževanjem ali s splošno dosegljivimi informacijami (npr. na intranetu, z okrožnicami ali dokumenti)	51%	46%	69%	83%

Tabela 9: Seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih, po velikosti podjetja, leto 2010 (vir: SURS)

Med podjetji v finančnem sektorju (tabela 10) je v letu 2010 v povprečju 95% podjetij seznanilo svoje uslužbence z njihovimi obveznostmi glede varne uporabe IKT. Pri tem so srednja in velika podjetja v finančnem sektorju 100% seznanila svoje zaposlene glede varne uporabe IKT. Zanimivo je to, da je z obveznim izobraževanjem to storilo 36% malih podjetij, 80% srednjih podjetij in samo 74% velikih podjetij.

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
Podjetja seznanila uslužbence z njihovimi obveznostmi glede varne uporabe IKT	95%	88%	100%	100%
..z obveznim izobraževanjem ali predstavitvami	59%	36%	80%	74%
..pri podpisu pogodbe, npr. pogodbe o zaposlitvi	90%	76%	100%	100%
..s prostovoljnim izobraževanjem ali s splošno dosegljivimi informacijami (npr. na intranetu, z okrožnicami ali dokumenti)	88%	z	z	100%

Tabela 10: Seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih v finančnem sektorju, leto 2010 (vir: SURS)

Pri podatkih v tabeli 10 se za velika podjetja v finančnem sektorju pojavi pomislek o relevantnosti statističnih podatkov, saj podatki odstopajo od podatkov za ostale kategorije podjetij. Pri vseh ostalih kategorijah podjetij se namreč pojavi pozitivna korelacija med sprejetimi formalnimi strategijami za varno uporabo IKT in seznanitvijo uslužbencev glede varne uporabe IKT, tu pa je ravno obratno. Sprejetih strategij je manj, seznanitev uslužbencev pa je stoodstotna.

4.4.2 Pregled statističnih podatkov glede na SKD

V finančnem sektorju ni na voljo vseh podatkov (tabela 11), vendar vidimo, da so podjetja na področju »Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade« seznanila uslužbence v 100%, vendar le v 46% z obveznim izobraževanjem ali predstavitvami. Zanimivo bi bilo narediti primerjavo s posledicami incidentov za ta podjetja, vendar nam za takšno primerjavo pri incidentih manjkajo potrebni podatki oziroma so le-ti zaupni (oznaka "z" v tabeli).

	64.19, 64.92 Drugo denarno posredništvo, drugo kreditiranje	65.1, 65.2 Dejavnost zavarovanja, pozavarovanja	66.12, 66.19 Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade
Podjetja seznanila uslužbence z njihovimi obveznostmi glede varne uporabe IKT	z	z	100%
..z obveznim izobraževanjem ali predstavitvami	70%	53%	46%
..pri podpisu pogodbe, npr. pogodbe o zaposlitvi	z	84%	z
..s prostovoljnim izobraževanjem ali s splošno dosegljivimi informacijami (npr. na intranetu, z okrožnicami ali dokumenti)	z	84%	z

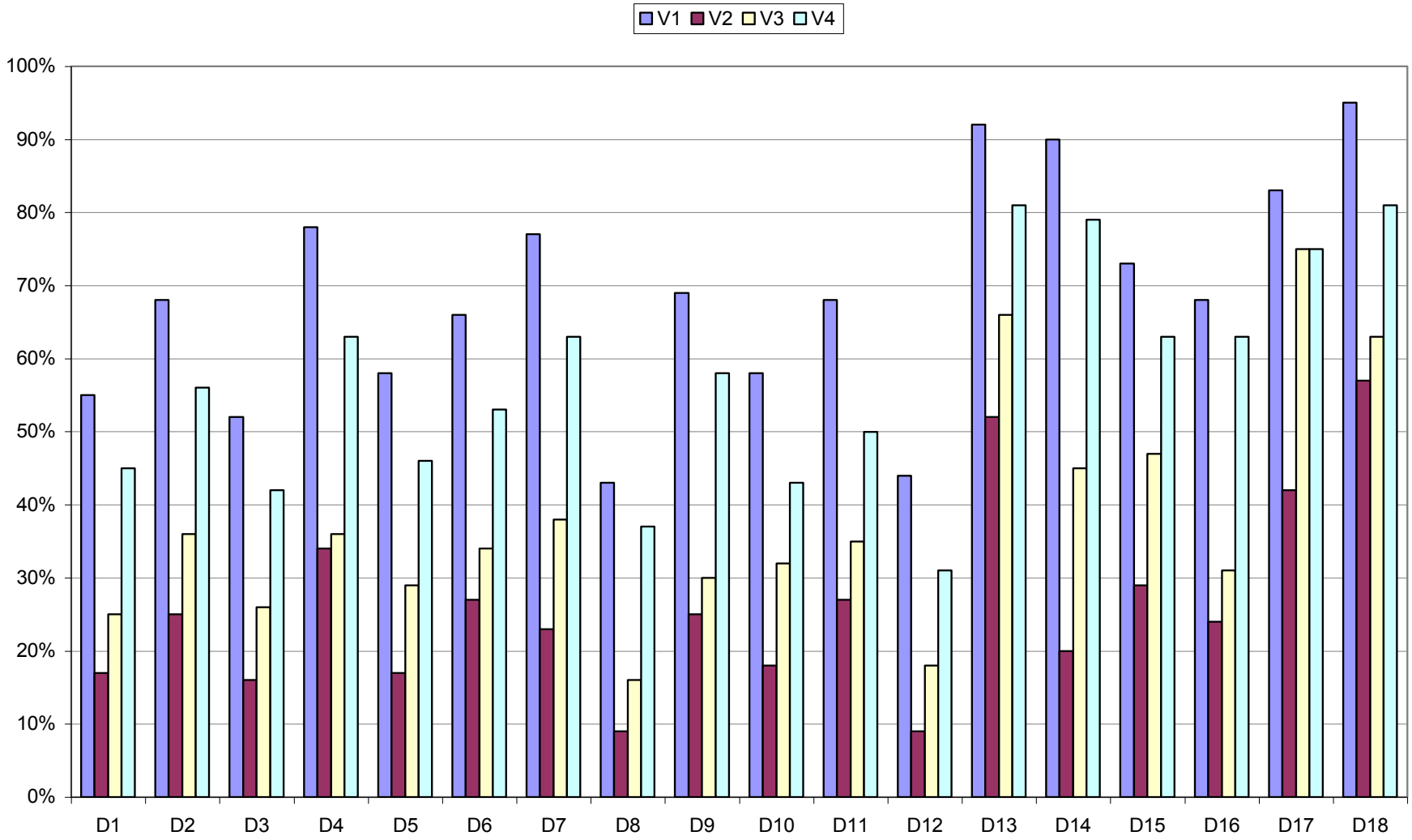
Tabela 11: Seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih v finančnem sektorju glede na SKD, leto 2010 (vir: SURS)

Legenda SKD →	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18
V1: Podjetja seznanila uslužbence z obveznostmi o varni uporabi IKT	55%	68%	52%	78%	58%	66%	77%	43%	69%	58%	68%	44%	92%	90%	73%	68%	83%	95%
V2: ..z obveznim izobraževanjem ali predstavitvami	17%	25%	16%	34%	17%	27%	23%	9%	25%	18%	27%	9%	52%	20%	29%	24%	42%	57%
V3: ..pri podpisu pogodbe, npr. pogodbe o zaposlitvi	25%	36%	26%	36%	29%	34%	38%	16%	30%	32%	35%	18%	66%	45%	47%	31%	75%	63%
V4: ..s prostovoljnim izobraževanjem ali s splošno dosegljivimi informacijami (npr. na intranetu, z okrožnicami ali dokumenti)	45%	56%	42%	63%	46%	53%	63%	37%	58%	43%	50%	31%	81%	79%	63%	63%	75%	81%

Tabela 12: Seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih po SKD, leto 2010 (vir: SURS)

Legenda dejavnosti:

D1 Proizvodne dejavnosti (dejavnosti C–F)
D2 Storitvene dejavnosti (dejavnosti G–S)
D3 10–18 Predelovalne dejavnosti (proizvodnja živil, tekstilnih, lesnih, papirnatih izdelkov, tiskarstvo)
D4 19–23 Predelovalne dejavnosti (proizvodnja naftnih, kemičnih, farmacevtskih surovin, izdelkov iz gume, plastičnih mas, nekovinskih mineralnih izdelkov)
D5 24–25 Predelovalne dejavnosti (proizvodnja kovin, nekovin)
D6 26–33 Predelovalne dejavnosti (proizvodnja računalnikov, elektronskih izdelkov, strojev, vozil, električnih naprav)
D7 35–39 Oskrba z energijo, vodo, ravnanje z odpadki
D8 41–43 Gradbeništvo
D9 45–47 Trgovina, vzdrževanje in popravila motornih vozil
D10 49–53 Promet in skladiščenje
D11 55 Gostinske nastanitvene dejavnosti, strežba jedi in pijač
D12 56 Dejavnost strežbe jedi in pijač
D13 58–63 Informacijske in komunikacijske dejavnosti
D14 68 Poslovanje z nepremičninami
D15 69–74 Strokovne, znanstvene in tehnične dejavnosti (sem spadajo tudi Pravne dejavnosti, Pravne in računovodske dejavnosti)
D16 77–82 Druge raznovrstne poslovne dejavnosti
D17 95 Druge dejavnosti: Popravila računalnikov in izdelkov za široko rabo
D18 Sektor IKT



Slika 15: Graf - seznanitev uslužbencev z njihovimi obveznostmi glede varne uporabe IKT v podjetjih po SKD, leto 2010 (vir: SURS)

Na področju ostalih SKD (tabela 12) so bila najbolj uspešna s seznanjanjem zaposlenih o varni uporabi IKT prav podjetja, ki delujejo v IKT sektorju. Najmanj podjetij (43%) je zaposlene seznanilo o varni uporabi IKT v gradbenem sektorju, s 44% je sledila dejavnost strežbe jedi in pijač.

4.4.3 Ugotovitve

Iz zbranih tabel je razvidna povezava med izdelano formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled ter seznanitvijo zaposlenih o varni uporabi IKT. To je razumljivo, kajti če ni vzpostavljene strategije za varno uporabo IKT, tudi ni neke osnove za seznanjanje zaposlenih.

4.5 Uporaba internih varnostnih pripomočkov ali postopkov v slovenskih podjetjih

4.5.1 Pregled statističnih podatkov glede na velikost podjetij

48% podjetij je v januarju 2010 kot interni varnostni pripomoček uporabljalo overjanje in avtorizacijo uporabnika s strojno opremo (npr. s pametnimi karticami). Močna gesla za avtentikacijo (geslo iz najmanj 8 različnih znakov in z veljavnostjo do šest mesecev, šifriran prenos in hranitev) je uporabljalo 41% podjetij (tabela 13).

37% podjetij je hranilo varnostne kopije podatkov na drugem kraju, 19% podjetij je vodilo dnevnik o aktivnostih informacijskega sistema in uporabnikov za analiziranje varnostnih incidentov. Le 3% podjetij je uporabljalo overjanje uporabnikov z biometričnimi metodami.

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
Močno geslo za avtentikacijo uporabnika[12]	41%	37%	56%	68%
Overjanje in avtorizacija uporabnika s strojno opremo (npr. pametne kartice)	48%	48%	50%	50%
Overjanje uporabnikov z biometričnimi metodami	3%	3%	4%	12%
Hranjenje varnostne kopije podatkov podjetja na drugem kraju	37%	33%	51%	67%
Vodenje dnevnika o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov	19%	15%	33%	47%

Tabela 13: Uporaba internih varnostnih pripomočkov ali postopkov v podjetjih za leto 2010 (vir: SURS)

V finančnem sektorju je uporaba varnostnih pripomočkov znatno višja, saj je močno geslo za avtentikacijo uporabljalo kar 86% podjetij, 83% podjetij je kot interni varnostni pripomoček uporabljalo overjanje in avtorizacijo uporabnika s

[12] Močno geslo za avtentikacijo uporabnika pomeni geslo iz najmanj 8 različnih znakov, veljavnost do šest mesecev, šifriran prenos in hranitev.

strojno opremo (npr. pametne kartice). Kar 90% podjetij je uporabljalo hranjenje varnostne kopije podatkov podjetja na drugem kraju. 75% podjetij je tudi vodilo dnevnik o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov.

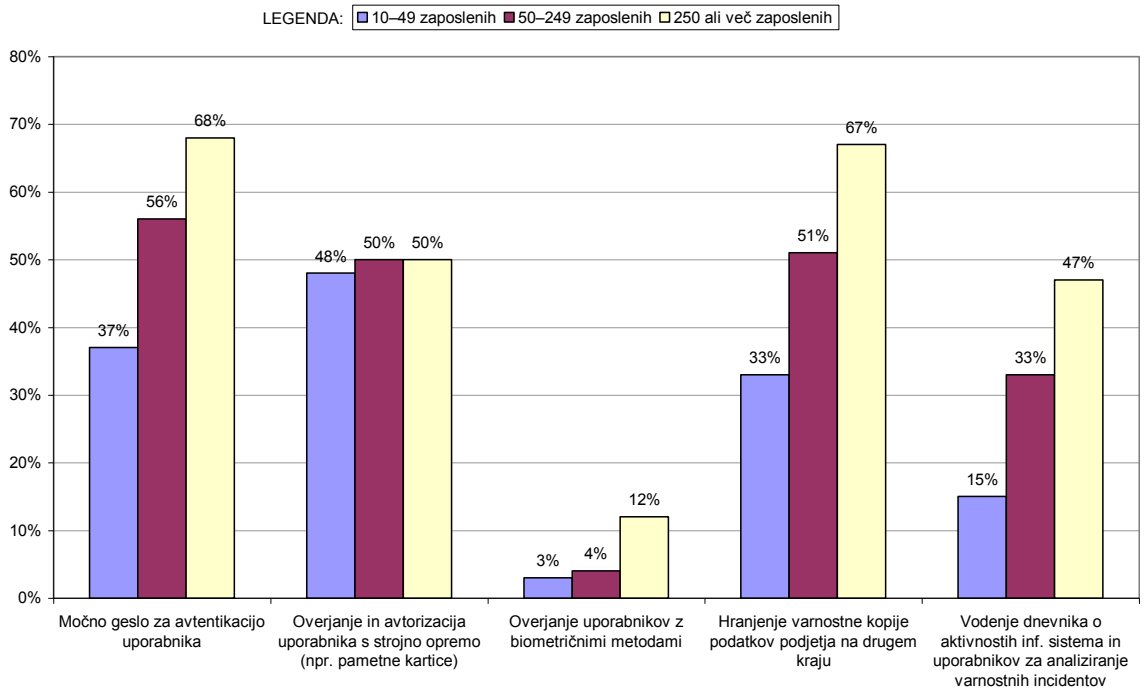


Tabela 14: Graf - uporaba internih varnostnih pripomočkov ali postopkov v podjetjih po velikosti podjetja za leto 2010 (vir: SURS)

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
Močno geslo za avtentikacijo uporabnika	86%	80%	z	z
Overjanje in avtorizacija uporabnika s strojno opremo (npr. pametne kartice)	83%	z	z	89%
Overjanje uporabnikov z biometričnimi metodami	8%	z	z	z
Hranjenje varnostne kopije podatkov podjetja na drugem kraju	90%	z	z	100%
Vodenje dnevnika o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov	75%	64%	z	z

Tabela 15: Uporaba internih varnostnih pripomočkov ali postopkov za podjetja v finančnem sektorju za leto 2010 (vir: SURS)

4.5.2 Pregled statističnih podatkov glede na SKD

V finančnem sektorju zopet opazimo "negativen" trend dejavnosti »Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade«, kjer samo 69% podjetij uporablja močno geslo za avtentikacijo uporabnika ter jih samo 62%

vodi dnevnik o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov (tabela 16).

	64.19, 64.92 Drugo denarno posredništvo, drugo kreditiranje	65.1, 65.2 Dejavnost zavarovanja, pozavarovanja	66.12, 66.19 Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade
Močno geslo za avtentikacijo uporabnika	100%	79%	69%
Overjanje in avtorizacija uporabnika s strojno opremo (npr. pametne kartice)	z	79%	z
Overjanje uporabnikov z biometričnimi metodami	z	z	z
Off site sistem (hranjenje varnostne kopije podatkov podjetja na drugem kraju)	z	84%	z
Vodenje dnevnika o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov	85%	68%	62%

Tabela 16: Uporaba internih varnostnih pripomočkov ali postopkov v podjetjih v finančnem sektorju po SKD, leto 2010 (vir: SURS)

Med ostalimi dejavnostmi (tabela 17) močno geslo za avtentikacijo najmanjkrat uporabijo v predelovalni dejavnosti (D3, 29%), sledita gradbeništvo (D8) in dejavnost strežbe jedi in pijač (D12).

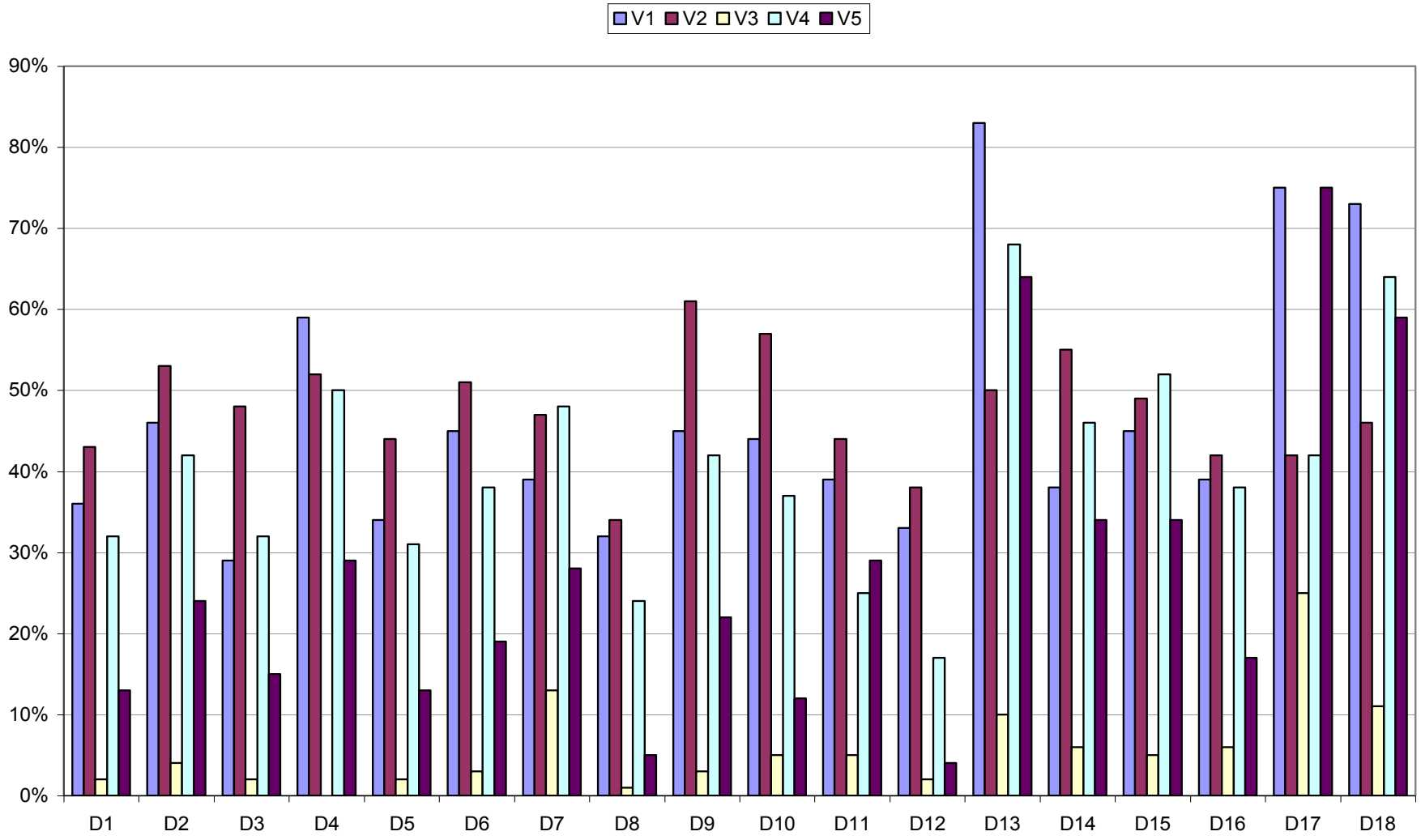
Med »varnejšimi« so IKT dejavnosti (D13) kjer 83% podjetij uporablja močno geslo za avtentikacijo in v kar 68% uporabljajo hranjenje varnostne kopije podatkov podjetja na drugem kraju.

	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18
V1: Močno geslo za avtentikacijo uporabnika	36%	46%	29%	59%	34%	45%	39%	32%	45%	44%	39%	33%	83%	38%	45%	39%	75%	73%
V2: Overjanje in avtorizacija uporabnika s strojno opremo (npr. pametne kartice)	43%	53%	48%	52%	44%	51%	47%	34%	61%	57%	44%	38%	50%	55%	49%	42%	42%	46%
V3: Overjanje uporabnikov z biometričnimi metodami	2%	4%	2%	-	2%	3%	13%	1%	3%	5%	5%	2%	10%	6%	5%	6%	25%	11%
V4: Hranjenje varnostne kopije podatkov podjetja na drugem kraju)	32%	42%	32%	50%	31%	38%	48%	24%	42%	37%	25%	17%	68%	46%	52%	38%	42%	64%
V5: Vodenje dnevnika o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov	13%	24%	15%	29%	13%	19%	28%	5%	22%	12%	29%	4%	64%	34%	34%	17%	75%	59%

Tabela 17: Uporaba internih varnostnih pripomočkov ali postopkov v podjetjih po SKD, leto 2010 (vir: SURS)

Legenda dejavnosti:

D1 Proizvodne dejavnosti (dejavnosti C–F)
D2 Storitvene dejavnosti (dejavnosti G–S)
D3 10–18 Predelovalne dejavnosti (proizvodnja živil, tekstilnih, lesnih, papirnatih izdelkov, tiskarstvo)
D4 19–23 Predelovalne dejavnosti (proizvodnja naftnih, kemičnih, farmacevtskih surovin, izdelkov iz gume, plastičnih mas, nekovinskih mineralnih izdelkov)
D5 24–25 Predelovalne dejavnosti (proizvodnja kovin, nekovin)
D6 26–33 Predelovalne dejavnosti (proizvodnja računalnikov, elektronskih izdelkov, strojev, vozil, električnih naprav)
D7 35–39 Oskrba z energijo, vodo, ravnanje z odpadki
D8 41–43 Gradbeništvo
D9 45–47 Trgovina, vzdrževanje in popravila motornih vozil
D10 49–53 Promet in skladiščenje
D11 55 Gostinske nastanitvene dejavnosti, strežba jedi in pijač
D12 56 Dejavnost strežbe jedi in pijač
D13 58–63 Informacijske in komunikacijske dejavnosti
D14 68 Poslovanje z nepremičninami
D15 69–74 Strokovne, znanstvene in tehnične dejavnosti (sem spadajo tudi Pravne dejavnosti, Pravne in računovodske dejavnosti)
D16 77–82 Druge raznovrstne poslovne dejavnosti
D17 95 Druge dejavnosti: Popravila računalnikov in izdelkov za široko rabo
D18 Sektor IKT



Slika 16:Graf - uporaba internih varnostnih pripomočkov ali postopkov v podjetjih po SKD, leto 2010 (vir: SURS)

4.5.3 Ugotovitve in priporočila za slovensko gospodarstvo

V tabeli 13 je pozornost vzbudila zadnja vrstica, ki predstavlja »vodenje dnevnika o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov«. Tu vidimo, da mala podjetja vodijo dnevnik v 15%, srednja v 34% ter velika v 47% primerov. Na podlagi navedenega je mogoče sklepati, da je pri velikih podjetjih verjetnost, da bodo zaznala varnostni incident trikrat višja kot pri malih podjetjih. Pojavi se vprašanje, ali morda mala in srednja podjetja ravno zaradi tega izmerijo tudi sorazmerno manjše število incidentov. To bi lahko pomenilo, da so morda v resnici mala in srednja podjetja imela več incidentov, kot kažejo statistični podatki.

Pri uporabi internih varnostnih pripomočkov negativno izstopa tudi dejavnost D15 (69–74 strokovne, znanstvene in tehnične dejavnosti), kamor spadajo tudi pravne dejavnosti ter pravne in računovodske dejavnosti. Samo 45% (le 4% nad povprečjem) podjetij v tej skupini je v letu 2010 uporabljalo močno geslo za overjanje, samo 52% jih uporablja hranjenje varnostne kopije podatkov podjetja na drugem kraju in samo 34% jih je vodilo dnevnik o aktivnostih inf. sistema in uporabnikov za analiziranje varnostnih incidentov. Po oceni, glede na podatke v tabeli 2 je leta 2010 med 4% in 17% teh podjetij in organizacij doživelo IKT varnostni incident s posledicami. V letu 2010 je le vsako peto podjetje na področju dejavnosti "69–74 strokovne, znanstvene in tehnične dejavnosti" imelo urejeno formalno strategijo za varno uporabo IKT z načrtom za njen redni pregled. Samo vsako peto podjetje v tej skupini dejavnosti je v letu 2010 seznanilo uslužbence z njihovimi obveznostmi glede varne uporabe IKT z obveznim izobraževanjem ali predstavitvami.

Potrebno se je zavedati, da predvsem večje pravne pisarne in računovodske organizacije razpolagajo z veliko količino zaupnih dokumentov in finančnih transakcij svojih strank. Verjetno so ravno zaradi slabega zavedanja o varnosti IKT v zadnjih letih pogosta tarča kriminalnih združb po vsem svetu. Te preko izkoriščanja ranljivosti v sistemih, šibkih gesel in nizkega zavedanja o grožnjah IKT zaposlenih v teh dejavnostih pridejo do zaupnih dokumentov in informacij o transakcijah njihovih strank [84]. To jim služi kot osnova za nadaljnje delovanje, informacije o prevzemih podjetij in gospodarsko vohunjenje. Posebej so na udaru velike pravne pisarne, ki imajo podružnice v več državah, kajti pogosto ta podjetja uporabljajo centralno hrambo dokumentov.

Priporočila:

Podjetja v SKD 69–74 (strokovne, znanstvene in tehnične dejavnosti) naj se glede varnostnih mehanizmov IKT zgledujejo po podjetjih v finančnem sektorju. Prav podjetja v finančnem sektorju (banke, zavarovalnice, borznoposredniške hiše) so pogosto naročniki pravnih storitev, zato bi morala pred začetkom sodelovanja preveriti skladnost z varnostnimi standardi pravnih pisarn in ostalih institucij, s katerimi imajo namen poslovno sodelovati.

4.6 Obseg uporabe odprtokodne programske opreme v slovenskih podjetjih

4.6.1 Uvod

V tem poglavju bom opravil analizo statističnih podatkov o uporabi odprtokodne programske opreme v slovenskih podjetjih v letu 2011. Skušal bom ugotoviti, ali obstaja povezava med posledicami incidentov ter uporabo odprtokodne programske opreme v slovenskih podjetjih.

4.6.2 Pregled statističnih podatkov glede na velikost podjetja

V tabeli 18 vidimo, da je bilo januarja 2011 med podjetji z najmanj 10 zaposlenimi osebami 71% takih, ki so uporabljala odprtokodno programsko opremo (npr. odprtokodni operacijski sistem, brskalnik, pisarniško programsko opremo itd.). Delež takih podjetij je bil glede na velikost podjetja (po številu zaposlenih oseb) največji med velikimi podjetji (250 ali več zaposlenih oseb), znašal pa je 79 %.

Največ podjetij (64%) je uporabljalo odprtokodne spletne brskalnike (npr. Mozilla Firefox, Google Chrome), 37% podjetij je uporabljalo odprtokodne pisarniške programske pakete, 18% podjetij pa odprtokodne operacijske sisteme (npr. Linux, Android). Takih podjetij je bilo največ med velikimi podjetji, in sicer 61%.

V tabeli 18 jasno vidimo trend povečevanja uporabe odprtokodne programske opreme z rastjo organizacije. Zelo očitna je rast odstotka uporabe odprtokodnih operacijskih sistemov od malih podjetij (14%), preko srednjih velikih podjetij (28%) do velikih podjetij (61%). Podoben trend se kaže pri uporabi odprtokodne PO za spletne strežnike (8%, 18%, 44%). Pri drugi PO, kot so strežniki za e-pošto, varnostne rešitve, e-učilnice ipd., je trend manj izrazit (20%, 21%, 41%), toda podatki kažejo, da velika podjetja v povprečju uporabljajo tovrstno odprtokodno PO dvakrat pogosteje kot manjša podjetja.

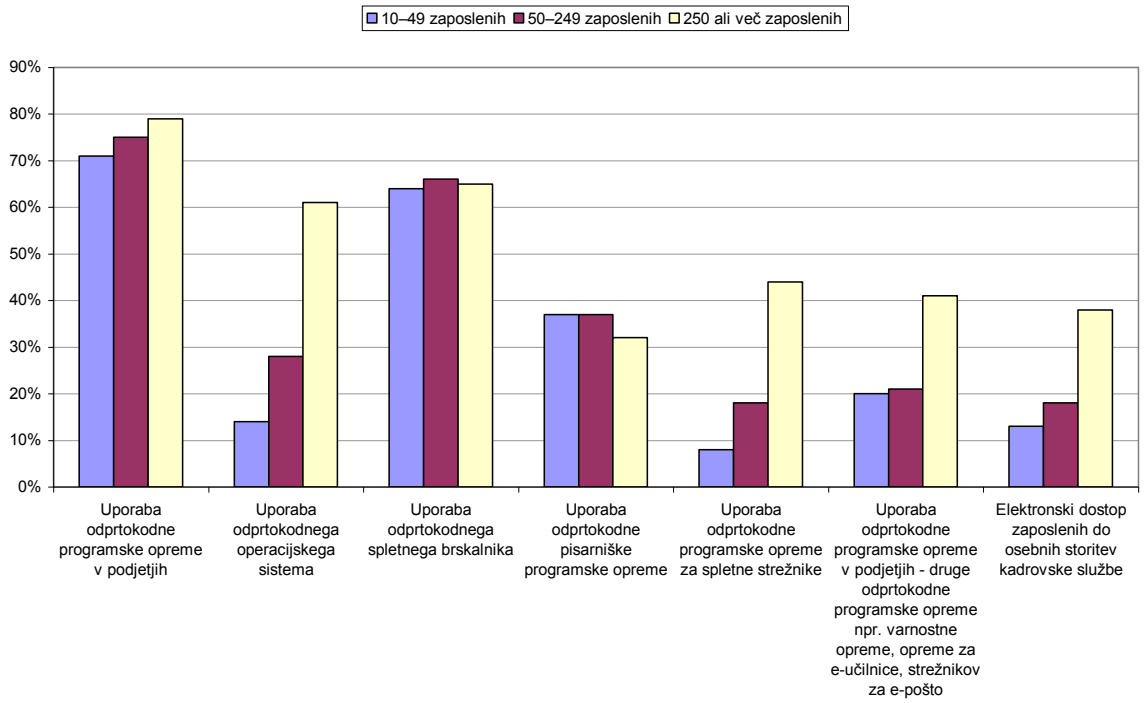
84% podjetij finančnega sektorja je v januarju 2011 uporabljalo odprtokodno programsko opremo. Tudi pri finančnih podjetjih je bila najpogostejša uporaba odprtokodnega spletnega brskalnika - uporabljalo ga je 67% teh podjetij, to je toliko kot v podjetjih v drugih dejavnostih. Sledila je uporaba odprtokodnega operacijskega sistema (56% podjetij), odprtokodne programske opreme za spletne strežnike (47% podjetij) ter uporaba druge odprtokodne programske opreme (npr. varnostna oprema, oprema za e-učilnice itd.). 26 % podjetij finančnega sektorja je uporabljalo odprtokodno pisarniško opremo (tabela 19).

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
Uporaba odprtokodne programske opreme v podjetjih	72%	71%	75%	79%
Uporaba odprtokodnega operacijskega sistema	18%	14%	28%	61%
Uporaba odprtokodnega spletnega brskalnika	64%	64%	66%	65%
Uporaba odprtokodne pisarniške programske opreme	37%	37%	37%	32%
Uporaba odprtokodne programske opreme za spletne strežnike	11%	8%	18%	44%
Uporaba odprtokodne programske opreme v podjetjih - druge odprtokodne programske opreme npr. varnostne opreme, opreme za e-učilnice, strežnikov za e-pošto	21%	20%	21%	41%
Elektronski dostop zaposlenih do osebnih storitev kadrovske službe	15%	13%	18%	38%

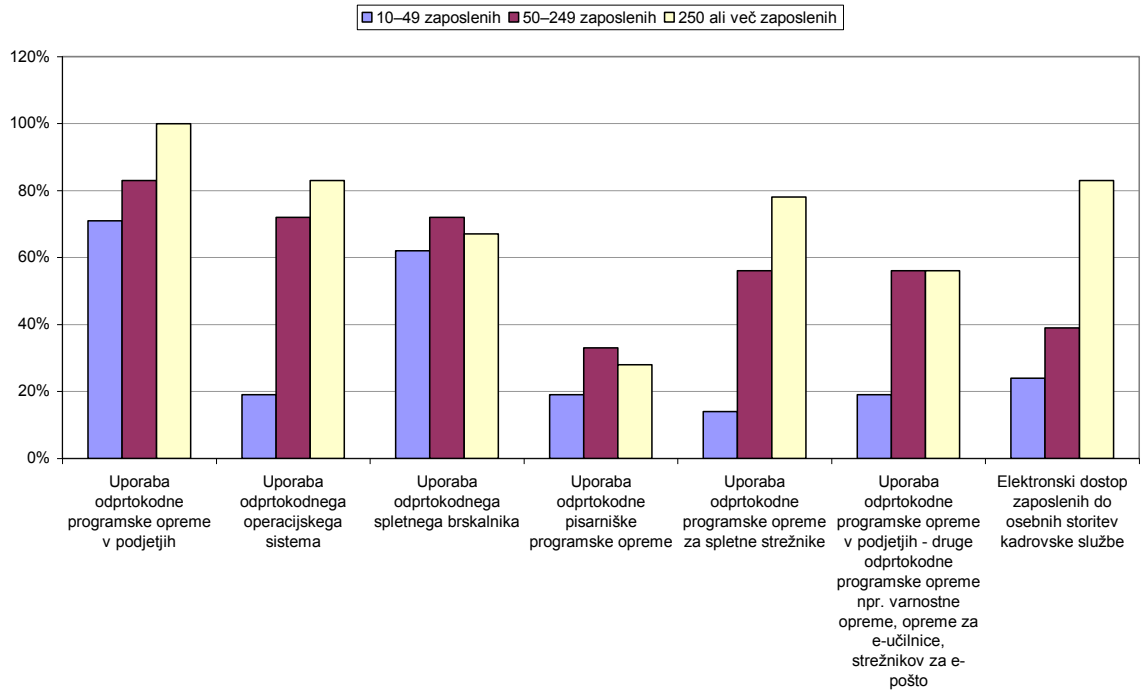
Tabela 18: Uporaba programske opreme v podjetjih po velikosti, leto 2011 (vir: SURS)

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
Uporaba odprtokodne programske opreme v podjetjih	84%	71%	83%	100%
Uporaba odprtokodnega operacijskega sistema	56%	19%	72%	83%
Uporaba odprtokodnega spletnega brskalnika	67%	62%	72%	67%
Uporaba odprtokodne pisarniške programske opreme	26%	19%	33%	28%
Uporaba odprtokodne programske opreme za spletne strežnike	47%	14%	56%	78%
Uporaba odprtokodne programske opreme v podjetjih - druge odprtokodne programske opreme npr. varnostne opreme, opreme za e-učilnice, strežnikov za e-pošto	42%	19%	56%	56%
Elektronski dostop zaposlenih do osebnih storitev kadrovske službe	47%	24%	39%	83%

Tabela 19: Uporaba programske opreme v podjetjih v finančnem sektorju po velikosti podjetja, leto 2011 (vir: SURS)



Slika 17:Graf - uporaba programske opreme v podjetjih po velikosti podjetja, leto 2011 (vir: SURS)



Slika 18:Graf - uporaba programske opreme v podjetjih v finančnem sektorju po velikosti podjetja, leto 2011 (vir: SURS)

4.6.3 Pregled statističnih podatkov glede na SKD

V finančnem sektorju so odprtokodno programsko opremo najmanj uporabljala podjetja v skupini dejavnosti »dejavnost zavarovanja, pozavarovanja« (79% podjetij).

Podjetja v dejavnosti »Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade« so le v 27% uporabljala odprtokodni operacijski sistem (tabela 20).

	64.19, 64.92 Drugo denarno posredništvo, drugo kreditiranje	**65.1, 65.2 Dejavnost zavarovanja, pozavarovanja**	**66.12, 66.19 Posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade**
Uporaba odprtokodne programske opreme v podjetjih	89%	79%	82%
Uporaba odprtokodnega operacijskega sistema	70%	53%	27%
Uporaba odprtokodnega spletnega brskalnika	74%	53%	73%
Uporaba odprtokodne pisarniške programske opreme	26%	42%	-
Uporaba odprtokodne programske opreme za spletne strežnike	59%	58%	-
Uporaba druge odprtokodne programske opreme npr. varnostne opreme, oprema za e-učilnice, strežnikov za e-pošto	56%	26%	36%
Elektronski dostop zaposlenih do osebnih storitev kadrovske službe	52%	53%	27%

Tabela 20: Uporaba programske opreme IKT v podjetjih v finančnem sektorju po SKD, leto 2011 (vir: SURS)

Glede na dejavnost podjetja v tabeli 21 vidimo, da je bil delež podjetij, ki so uporabljala odprtokodno programsko opremo, večji med podjetji v storitvenih dejavnostih (75%) kot med podjetji v proizvodnih dejavnostih (69%). Uporaba odprtokodnega spletnega brskalnika prevladuje v vseh podjetjih, ne glede na dejavnost (67% med podjetji v storitvenih in 61 % v proizvodnih dejavnostih) in 95% v sektorju IKT ter D13 (informacijske in komunikacijske dejavnosti).

Na sliki 19 vidimo graf uporabe odprtokodne PO po dejavnostih. Zaradi lažje primerjave so v desnem delu dodane še dejavnosti D19, D20 in D21, ki predstavljajo naslednje dejavnosti:

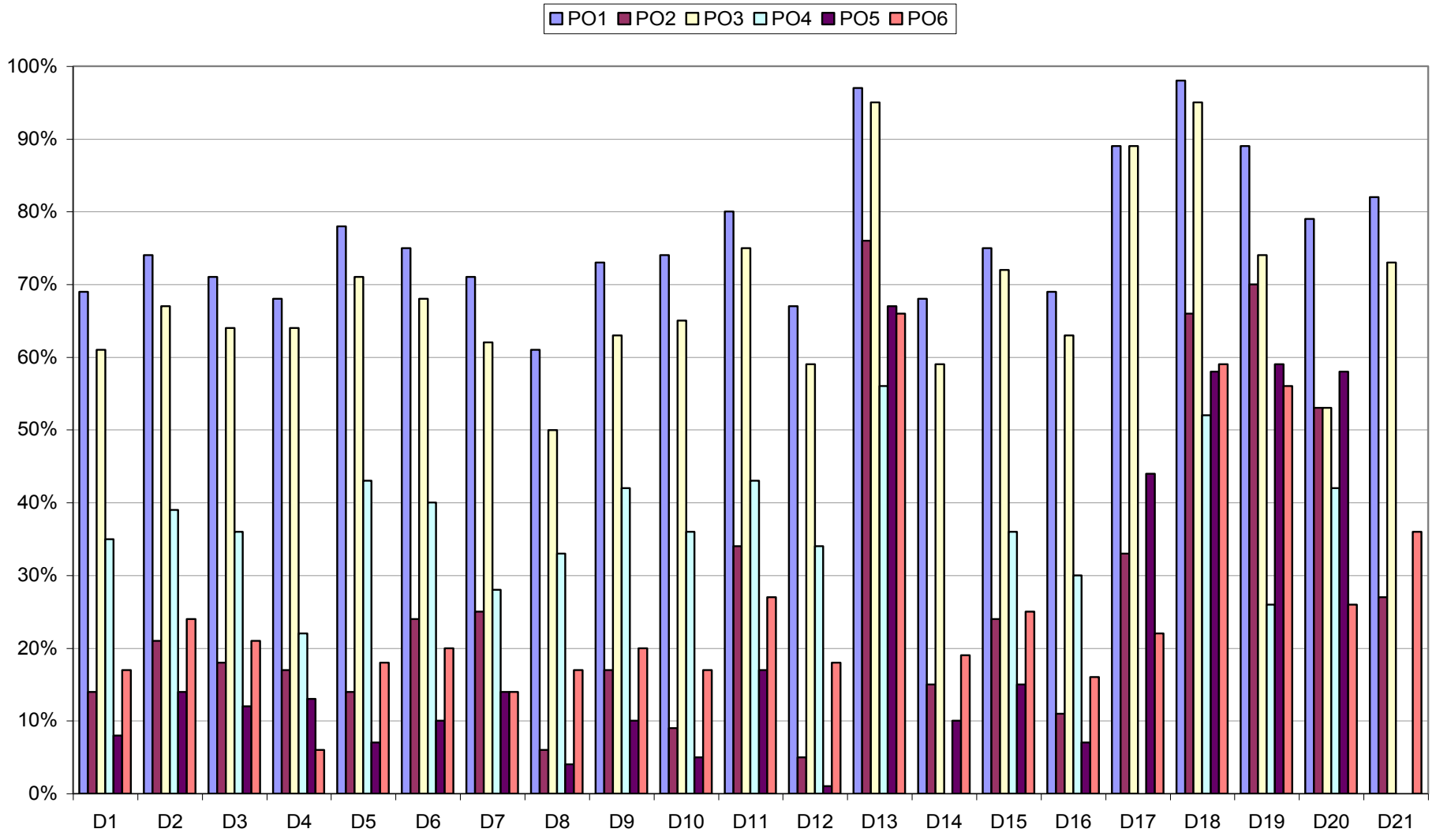
- D19 - 64.19, 64.92 drugo denarno posredništvo, drugo kreditiranje;
- D20 - 65.1, 65.2 dejavnost zavarovanja, pozavarovanja;
- D21 - 66.12, 66.19 posredništvo pri trgovanju z vrednostnimi papirji in borznim blagom, druge pomožne dejavnosti za finančne storitve, razen za zavarovalništvo in pokojninske sklade.

	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18
PO1: Uporaba odprtokodne programske opreme v podjetjih	69%	74%	71%	68%	78%	75%	71%	61%	73%	74%	80%	67%	97%	68%	75%	69%	89%	98%
PO2: Uporaba odprtokodnega operacijskega sistema	14%	21%	18%	17%	14%	24%	25%	6%	17%	9%	34%	5%	76%	15%	24%	11%	33%	66%
PO3: Uporaba odprtokodnega spletnega brskalnika	61%	67%	64%	64%	71%	68%	62%	50%	63%	65%	75%	59%	95%	59%	72%	63%	89%	95%
PO4: Uporaba odprtokodne pisarniške programske opreme	35%	39%	36%	22%	43%	40%	28%	33%	42%	36%	43%	34%	56%	0%	36%	30%	0%	52%
PO5: Uporaba odprtokodne programske opreme za spletne strežnike	8%	14%	12%	13%	7%	10%	14%	4%	10%	5%	17%	1%	67%	10%	15%	7%	44%	58%
PO6: Uporaba druge odprtokodne programske opreme npr. varnostne opreme, oprema za e-učilnice, strežnikov za e-pošto	17%	24%	21%	6%	18%	20%	14%	17%	20%	17%	27%	18%	66%	19%	25%	16%	22%	59%

Tabela 21: Uporaba odprtokodne programske opreme IKT v podjetjih po SKD, leto 2011 (vir: SURS)

Legenda dejavnosti:

D1 Proizvodne dejavnosti (dejavnosti C–F)
D2 Storitvene dejavnosti (dejavnosti G–S)
D3 10–18 Predelovalne dejavnosti (proizvodnja živil, tekstilnih, lesnih, papirnatih izdelkov, tiskarstvo)
D4 19–23 Predelovalne dejavnosti (proizvodnja naftnih, kemičnih, farmacevtskih surovin, izdelkov iz gume, plastičnih mas, nekovinskih mineralnih izdelkov)
D5 24–25 Predelovalne dejavnosti (proizvodnja kovin, nekovin)
D6 26–33 Predelovalne dejavnosti (proizvodnja računalnikov, elektronskih izdelkov, strojev, vozil, električnih naprav)
D7 35–39 Oskrba z energijo, vodo, ravnanje z odpadki
D8 41–43 Gradbeništvo
D9 45–47 Trgovina, vzdrževanje in popravila motornih vozil
D10 49–53 Promet in skladiščenje
D11 55 Gostinske nastanitvene dejavnosti, strežba jedi in pijač
D12 56 Dejavnost strežbe jedi in pijač
D13 58–63 Informacijske in komunikacijske dejavnosti
D14 68 Poslovanje z nepremičninami
D15 69–74 Strokovne, znanstvene in tehnične dejavnosti (sem spadajo tudi Pravne dejavnosti, Pravne in računovodske dejavnosti)
D16 77–82 Druge raznovrstne poslovne dejavnosti
D17 95 Druge dejavnosti: Popravila računalnikov in izdelkov za široko rabo
D18 Sektor IKT



Slika 19:Graf - uporaba odprtokodne programske opreme IKT v podjetjih po SKD, leto 2011 (vir: SURS)

4.6.4 Korelacija uporabe odprtokodne programske opreme s posledicami incidentov

Zanimalo me je, kako uporaba odprtokodne programske opreme korelira s posledicami incidentov. Za vhodne podatke sem izbral tabelo s posledicami incidentov po velikosti podjetij glede na število zaposlenih (tabela 1) ter uporabo programske opreme po velikosti podjetij (tabela 18). Spodaj navajam tabeli z vrednostmi, ki sem jih uporabil za določanje spremenljivk za preverjanje prej omenjene korelacije.

Tip incidenta	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
TI1: Nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi	5,3%	10,8%	19,3%
TI2: Nedosegljivost storitev IKT zaradi napada od zunaj	1,7%	1,7%	3,1%
TI3: Uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa	1,9%	5,4%	4,4%
TI4: Razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma	1,3%	1,3%	4,4%

Tabela 22: TAB1 - Posledice varnostnih incidentov, s katerimi so se srečala podjetja v letu 2010, po velikosti podjetja (vir: SURS)

Tip programske opreme	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
PO1: Uporaba odprtokodne programske opreme v podjetjih	71%	75%	79%
PO2: Uporaba odprtokodnega operacijskega sistema	14%	28%	61%
PO3: Uporaba odprtokodnega spletnega brskalnika	64%	66%	65%
PO4: Uporaba odprtokodne pisarniške programske opreme	37%	37%	32%
PO5: Uporaba odprtokodne programske opreme za spletne strežnike	8%	18%	44%
PO6: Uporaba odprtokodne programske opreme v podjetjih - druge odprtokodne programske opreme npr. varnostne opreme, opreme za e-učilnice, strežnikov za e-pošto	20%	21%	41%
PO7: Elektronski dostop zaposlenih do osebnih storitev kadrovske službe	13%	18%	38%

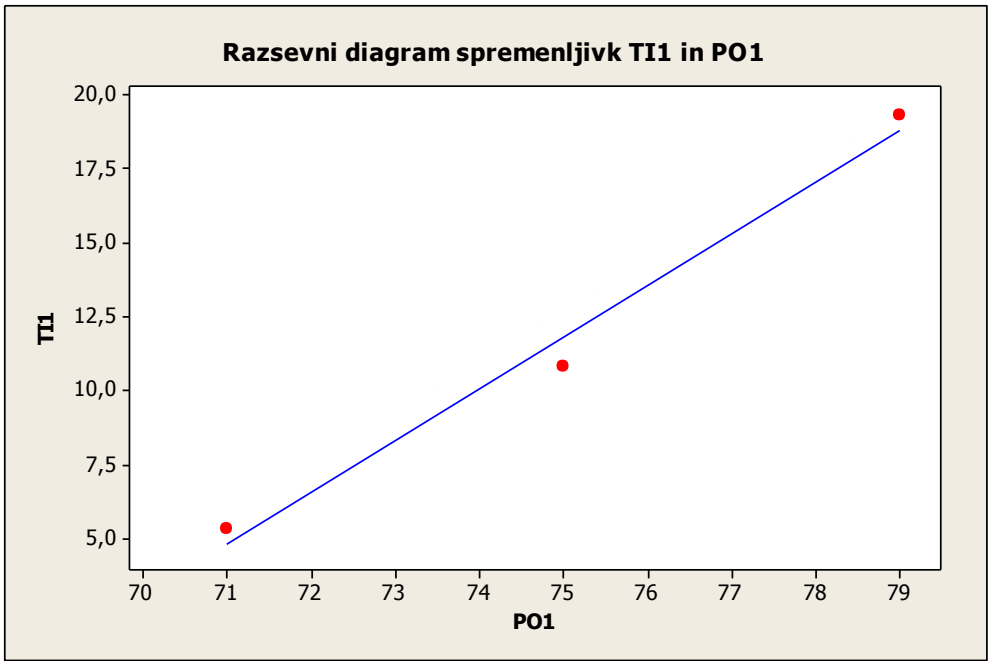
Tabela 23: TAB2 - Uporaba programske opreme v podjetjih po velikosti, leto 2011 (vir: SURS)

Za oceno korelacije sem uporabil Spearmanovo metodo, ki ne predpostavlja normalne porazdelitve podatkov [88].

Za uporabo omenjene metode morata biti izpolnjeni naslednji dve predpostavki.

1. Spremenljivki morata biti ordinalni, intervalni ali razmernostni. V našem primeru sta obe spremenljivki razmernostni (odstotki 0 do 100).
2. Med spremenljivkama mora obstajati monotona povezava. To pomeni, da če vrednost prve spremenljivke raste, mora naraščati tudi vrednost druge spremenljivke. Druga možnost je, da vrednost ene spremenljivke raste, vrednost druge spremenljivke pa pada. To je najbolje preveriti z razsevnim diagramom, ki grafično prikaže povezanost med dvema spremenljivkama. Podatki so prikazani kot zbirka točk, kjer ima vsaka točka vrednost dveh spremenljivk, kar določa njeno lego na abscisi in ordinati.

Primer preverjanja monotonega razmerja med TI1 in PO1 v programu Minitab [77] kaže slika 20. Slika jasno pokaže, da je razmerje monotono naraščajoče.



Slika 20: Razsevni diagram - preverjanje monotonosti spremenljivk TI1 in PO1 (program Minitab)

Korelacijska funkcija podaja tako imenovani Spearmanov ρ (ro). Ta ima lahko vrednost med -1,0 in +1,0. Bližje ko je vrednost +1,0, bolj primerjani spremenljivki pozitivno korelirata oziroma boljša linearna povezava obstaja med njima.

Stopnja (jakost, moč) povezanosti glede na vrednost korelacijskega koeficienta se običajno poimenuje po naslednji lestvici:

- 0,00: ni povezanosti;
- 0,01 - 0,19: neznatna povezanost;
- 0,20 - 0,39: nizka (šibka) povezanost;
- 0,40 - 0,59: srednja (zmerna) povezanost;
- 0,60 - 0,79: visoka (močna) povezanost;
- 0,80 - 0,99: zelo visoka povezanost;
- 1: popolna (funkcijska) povezanost.

Seveda pa visoka vrednost koeficienta korelacije še ne pomeni neposredne vzročno-posledične povezanosti, kajti dve spremenljivki lahko kažeta visoko stopnjo povezanosti, v realnem svetu pa nimata dejanske povezave. Na primer če sta zrasli vrednost borznega indeksa in prodaja prenosnih računalnikov, iz tega še ne moremo sklepati, da ljudje kupujejo prenosne računalnike, ker je zrasla vrednost borznega indeksa.

V nadaljevanju bom s pomočjo korelacijske funkcije preveril vsako vrstico iz tabele 22 z vsako vrstico tabele 23. Ker so vrednosti obeh spremenljivk razmernostne (med 0 in 100 odstotki) in imajo enako mersko lestvico (odstotki), s pomočjo Spearmanove korelacije dobim oceno, v kolikšni meri povečanje oziroma zmanjšanje vrednosti ene spremenljivke vpliva na povečanje oziroma zmanjšanje vrednosti druge spremenljivke.

Za izračun korelacije sem iz statističnih podatkov SURS priredil naslednji dve tabeli:

- tabela 22 - TAB1 (posledice varnostnih incidentov, s katerimi so se srečala podjetja v 2010) in
- tabela 23 - TAB2 (uporaba programske opreme v podjetjih po velikosti, leto 2011).

Vrednosti v obeh tabelah so s pretvorbo v odstotke normalizirane. Med zajemom ene in druge tabele je sicer preteklo približno eno leto, a predpostavimo, da se vrednosti niso bistveno spremenile. Na osnovi korelacije posameznih vrstic (neodvisnih statističnih spremenljivk) med tabelama želimo preveriti, ali med njima obstaja linearna povezava glede na velikost podjetja.

V TAB1 sem vrstice označil s TI1 do TI4. V TAB2 pa sem vrstice označil s PO1 do PO7. Korelacijo med posameznima vrsticama izračunam po Spearmanovi formuli r = r(TIx, POy) = r_{TIxPOy}. Če naredim korelacijo vsake vrtice v TAB1 z vsako vrstico v TAB2, dobim matriko v tabeli 24.

	TI1	**TI2**	**TI3**	**TI4**
PO1	r(TI1, PO1)	r(TI2, PO1)	r(TI3, PO1)	r(TI4, PO1)
PO2	r(TI1, PO2)	r(TI2, PO2)	r(TI3, PO2)	r(TI4, PO2)
PO3	r(TI1, PO3)	r(TI2, PO3)	r(TI3, PO3)	r(TI4, PO3)
PO4	r(TI1, PO4)	r(TI2, PO4)	r(TI3, PO4)	r(TI4, PO4)
PO5	r(TI1, PO5)	r(TI2, PO5)	r(TI3, PO5)	r(TI4, PO5)
PO6	r(TI1, PO6)	r(TI2, PO6)	r(TI3, PO6)	r(TI4, PO6)
PO7	r(TI1, PO7)	r(TI2, PO7)	r(TI3, PO7)	r(TI4, PO7)

Tabela 24: Matrika izračunanih Spearmanovih korelacijskih faktorjev

Izračun dejanske matrike korelacijskih faktorjev (tabela 25) sem izvedel v programu Minitab. Ta je za vsak faktor vrnil tudi faktor zaupanja p, ki je zapisan pod vsako vrednostjo ρ. Kjer se pojavi "*", to pomeni, da zaradi zelo visoke povezanosti dveh spremenljivk pride do deljenja z 0 in zato vrednosti ni moč izračunati.

Opomba: Vrednost faktorja zaupanja p=0,60 pomeni, da obstaja 60% možnost, da vrednost statistične spremenljivke odstopa (deviacija) od pričakovane vrednosti izključno zaradi naključja. Če je vrednost p=0,01, pa to pomeni, da obstaja le 1% možnosti, da je do deviacije prišlo zaradi naključja ter da so verjetno vključeni drugi dejavniki [64].

V matriki korelacijskih faktorjev (tabela 25) sem s sivim ozadjem v vsakem stolpcu označil celice s posledicami incidentov, ki imajo najvišjo stopnjo povezanosti z uporabo določenega tipa (odprtokodne) programske opreme (visoka povezanost). Termin "odprtokodne" sem namenoma dal v oklepaj, kajti uporaba določenega tipa programske opreme (spletni strežnik, e-poštni strežnik ipd.) ima že sama po sebi lahko pozitivno korelacijo v primerjavi s posledicami incidentov. Razlog za to je odpiranje (sredstev) virov informacij organizacije svetu, ki s sabo prinaša določena tveganja ne glede na to, ali gre za licenčno ali odprtokodno programsko opremo.

Na osnovi tega bi lahko sklepali na določeno povezanost med uporabo programske opreme določenega tipa in posledicami incidentov, vendar moramo te številke jemati zelo previdno, kajti kot sem že zapisal, teoretično izračunana močna povezanost še ne pomeni nujno tudi močne povezanosti v realnem svetu.

	TI1: nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi	**TI2:** nedosegljivost storitev IKT zaradi napada od zunaj	**TI3:** uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa	**TI4:** razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma
PO1: uporaba odprtokodne programske opreme v podjetjih	1,000 *	0,866 0,333	0,500 0,667	0,866 0,333
PO2: uporaba odprtokodnega operacijskega sistema	1,000 *	0,866 0,333	0,500 0,667	0,866 0,333
PO3: uporaba odprtokodnega spletnega brskalnika	0,500 0,667	0,000 1,000	1,000 *	0,000 1,000
PO4: uporaba odprtokodne pisarniške programske opreme	-0,866 0,333	-1,000 *	0,000 1,000	-1,000 *
PO5: uporaba odprtokodne programske opreme za spletne strežnike	1,000 *	0,866 0,333	0,500 0,667	0,866 0,333
PO6: uporaba odprtokodne programske opreme v podjetjih - druge odprtokodne programske opreme npr. varnostne opreme, opremo za e-učilnice, strežnikov za e-pošto	1,000 *	0,866 0,333	0,500 0,667	0,866 0,333
PO7: elektronski dostop zaposlenih do osebnih storitev kadrovske službe	1,000 *	0,866 0,333	0,500 0,667	0,866 0,333

Tabela 25: Spearmanova korelacija med posledicami incidentov ter uporabo odprtokodne programske opreme po velikosti podjetij

V nadaljevanju poskušam čimbolj realno ovrednotiti ocenjene korelacijske faktorje ρ, zbrane v tabeli 25.

1. Nedosegljivost storitev IKT, uničenje ali zlonamerno spreminjanje podatkov zaradi napake v programski ali strojni opremi

Tu je analiza pokazala, da najbolj korelira uporaba odprtokodne programske opreme v splošnem, sledita pa uporaba odprtokodnega operacijskega sistema ter uporaba odprtokodne programske opreme za spletne strežnike. Uporaba programske opreme za spletne strežnike je vedno na udaru, kajti napadalci najprej poskušajo pridobiti več informacij oziroma dostop preko »vrat«, ki so odprta svetu. To pa spletni strežniki z nameščeno programsko opremo zagotovo so. Na prvi pogled se zdi, da je odprtokodna programska oprema zelo na udaru, vendar je na odnos med programsko opremo (tudi strojno opremo) ter nevarnostjo incidentov potrebno gledati širše. Ne vemo, kako je bilo poskrbljeno za operacijski sistem, torej ali je bil pravilno in redno posodobljen ter ali je bil pravilno varnostno nastavljen. Enako velja za strežnike za e-pošto. Gotovo so podjetja, ki sploh ne uporabljajo spletnih strežnikov in strežnikov za e-pošto, v tem oziru bolj varna, vendar je danes takšno podjetje težko najti. Primer teoretično visoke korelacije, ki je ne moremo upoštevati, je elektronski dostop zaposlenih do osebnih storitev kadrovske službe. Če upoštevamo logične dejavnike, je jasno, da tu v realnem svetu ni tako močne povezave med takšnim elektronskim dostopom in nedosegljivostjo storitev IKT.

2. Nedosegljivost storitev IKT zaradi napada od zunaj

Tu se kaže visoka stopnja korelacije z uporabo odprtokodnega operacijskega sistema, odprtokodne programske opreme za spletne strežnike ter strežnike za e-pošto. Strežniki za e-pošto so zaradi same zasnove protokola, katerega zasnova izhaja iz začetkov interneta v osemdesetih letih prejšnjega stoletja, dokaj ranljivi za razne napade. Če niso pravilno nastavljeni, se da preko omrežja pridobiti uporabniška imena in gesla uporabnikov e-pošte, sam strežnik pa izkoristiti za pošiljanje neželene e-pošte. Ranljivim strežnikom za e-pošto sledijo že omenjeni spletni strežniki ter odprtokodni operacijski sistemi. To bomo preverili v nadaljevanju.

3. Uničenje ali zlonamerno spreminjanje podatkov zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa

Tu koeficient korelacije kaže zelo visoko povezanost z uporabo odprtokodnega spletnega brskalnika. To je razumljivo, saj zlonamerneži preko okuženih ali posebej pripravljenih spletnih strani prežijo na nič hudega sluteče obiskovalce in preko ranljivosti v brskalnikih izvedejo kodo za izkoriščanje ranljivosti, ki ima različne posledice. Mnogokrat gre za nalaganje zlonamerne programske opreme (virus, trojanski konj, program za beleženje tipkanja in za prestrezanje gesel (angl. keylogger). Vse aktivnosti pa merijo na pridobitev nedovoljenega dostopa in poskus ohranjanja le-tega. Zgolj zmerna povezanost se kaže pri uporabi odprtokodne programske opreme za spletne strežnike ter e-pošto.

4. Razkritje zaupnih podatkov v elektronski obliki s strani zaposlenih bodisi namenoma ali nenamenoma.
Tu so opazne tri zelo visoke povezanosti in pri vsaki je potreben širši pogled na problematiko.

Strežniki za e-pošto zaradi možnosti posredovanja informacij že sami po sebi predstavljajo grožnjo. Zavedati se je potrebno, da do razkritja podatkov lahko pride tudi zaradi napačno vnesenega elektronskega naslova prejemnika, ker je zaposleni prebiral službeno e-pošto na javno dostopnem računalniku, pri čemer obstaja možnost, da je nehote posredoval geslo zlonamernežu, ki je potem izkoristil ta dostop za dostop do službene e-pošte. Podobno velja za prebiranje e-pošte v primeru, da se je zaposleni s svojo mobilno napravo povezal na nevarovano brezžično dostopno točko, kjer je prišlo do prestrezanja seje ali pa kraje dostopa. Morda je zaposleni izgubil mobilno napravo, in ker ni bila primerno varovana, je zlonamernež imel lahek dostop do e-pošte.

Pri programski opremi za spletne strežnike lahko upoštevamo ranljivost opreme, saj je bil morebiti strežnik slabo zavarovan ali nastavljen (angl. insecure configuration), morda pa je zaposleni nehote posredoval informacije, ki ne bi smele biti dostopne javnosti.

Pri elektronskem dostopu do kadrovske službe obstaja tudi nevarnost kraje identitete. Na primer, nekdo se predstavi kot sodelavec ali vodja oddelka v podjetju ter preko e-pošte oziroma elektronskih obrazcev zaprosi za določene informacije. Kadrovnik mu nič hudega sluteč posreduje želene informacije (delovna doba, višina plače, bonitete, pogodba o zaposlitvi, preglednica delovne prisotnosti ipd.), vendar jih dobi »zlonamerna« oseba. V primeru da kadrovska služba uporablja namensko aplikacijo za olajšanje dela, obstaja verjetnost, da bo kdo od zaposlenih poskušal zaobiti varnostne mehanizme v aplikaciji in tako pridobiti podatke, ki jih sicer ne bi smel.

Ocena
V statističnih podatkih ni informacije, ali so podjetja, ki so doživela posledice incidentov, uporabljala odprtokodno programsko opremo in v kolikšni meri. Prav tako pri uporabi programske opreme ni nikjer navedeno, ali so ta podjetja uporabljala le odprtokodno programsko opremo ali tudi licenčno programsko opremo in v kolikšni meri. Zaradi tega je gornje ugotovitve potrebno jemati z rezervo. Menim namreč, da ugotovitve bolj kažejo na korelacijo posledic incidentov z uporabo določene programske opreme (e-poštni strežnik, spletni strežnik, brskalnik, pisarniški program ipd.), kot pa na večje tveganje pri uporabi odprtokodne programske opreme.

V petem poglavju bom prikazal podrobnejšo analizo izbrane odprtokodne PO in to odprtokodno PO na podlagi zaznanih ranljivosti v letu 2010 primerjal z licenčno PO istega tipa. Tako bomo lahko dejansko videli, v kolikšni meri teoretično odprtokodna PO v primerjavi z licenčno PO vpliva na število ter posledice incidentov.

4.7 Priporočila in smernice slovenskemu gospodarstvu

Trček je že leta 2006 navedel, da je človek največkrat najšibkejši člen v varovanju IKT [17]. Tudi nekateri raziskovalci so ocenjevali [8], da je v 80% za varnostne incidente kriv človeški faktor (slabo zavedanje in ravnanje na področju varnosti) in ne varnostna tehnologija.

Koristno bi bilo, da podjetja uvedejo izobraževanja o IKT in organizacijski varnosti kot del procesa, podobno kot morajo zakonsko zadostiti izobraževanju zaposlenih glede požarne varnosti in varstva pri delu.

Priporočam, da podjetja izvajajo naslednje aktivnosti za povečanje organizacijske varnosti in varnosti IKT:

1) obvezna izobraževanja o varni uporabi IKT in organizacijski varnosti za zaposlene vsaj enkrat letno;
2) management podjetij naj izboljša zavest o pomenu informacijske varnosti oziroma vzpostavi varnostno-organizacijsko kulturo po smernicah, opisanih v poglavju 3;
3) če organizacija še nima vpeljanega SUIV, naj ga čimprej vpelje.

Predlagam, da se v Sloveniji čimprej ponovno izvedejo raziskave, ki so obravnavane v poglavjih 4.2 do 4.6. Tako bo na osnovi analize teh podatkov moč videti napredek ter zaznati, kje vse še obstajajo pomanjkljivosti. Pri tem je potrebno upoštevati trenutne trende varnostnih IKT incidentov v svetu, predvsem v ZDA, ki je najbolj na udaru zaradi največje gostote povezane tehnologije IKT v korporativnem in zasebnem sektorju.

V raziskavi o uporabi programske opreme bi bilo potrebno bolje razdelati vrste programske opreme. Doda naj se tudi vprašanje, kako pogosto in na kakšen način podjetja skrbijo za posodabljanje sistemov IKT s popravki in koliko sistemov ne posodabljajo ter razloge, zakaj jih ne posodabljajo (licence, t.i. "legacy" programska oprema, strokovno osebje ipd.).

Menim, da bi morala Slovenija narediti podrobno statistično raziskavo o uporabi programske opreme, pri čemer bi morali pridobiti tudi bolj podrobne podatke o količini in vrsti odprtokodne ter licenčne programske opreme v uporabi po posameznih sektorjih (SKD).

Nekatere dejavnosti bi bilo potrebno obravnavati ločeno in ne v sklopu z drugimi dejavnostmi. Te dejavnosti so: zdravstvo, pravne storitve, pravni sektor, računovodski sektor ter vladni sketor in javna uprava.

Stolpec D15 (sem spadajo tudi pravne in računovodske dejavnosti) v tabeli 2 kaže, da so bile te dejavnosti že v letu 2010 pogosto tarča zunanjih napadov na njihove sisteme IKT.

Z bolj podrobnimi statističnimi podatki za naštete dejavnosti bi lahko na osnovi analize (razdelek 4.6.4) programske opreme, posledic in števila incidentov ter trendov v svetu bolje ter pravočasno predvideli in zavarovali najbolj izpostavljene sektorje ali podjetja.

5 Obravnava statističnih podatkov o uporabi PO z bazo ranljivosti CVE

5.1 Definicije

CVE (Common Vulnerabilities and Exposures) [66] je baza javno objavljenih ranljivosti in izpostavljenosti programske ter strojne opreme, ki jo upravlja organizacija MITRE. CVE je postal de facto standard in se uporablja za enolično identifikacijo ranljivosti, zato je splošno sprejet na področju varnosti. Uporaba CVE-jev kot identifikatorjev ranljivosti omogoča obdelavo informacij o ranljivosti med različnimi varnostnimi proizvodi in storitvami. Vsaka ranljivost v CVE bazi ima enoličen identifikator v obliki CVE-YYYY-nnnn. Pri tem je YYYY oznaka za leto, v katerem je bila prvič predlagana za objavo v CVE bazi, nnnn pa je zaporedna številka.

Problem pri uporabi identifikatorjev CVE za štetje ranljivosti je, da lahko en CVE zapis združuje več ranljivosti ali pa se ista ranljivost pojavi v več zapisih. To lahko vodi do manj natančnega števila ranljivosti.

Prav tako velja omeniti, da zaradi prevelikega števila ranljivosti v vseh vrstah programske in strojne opreme ter velikega števila proizvajalcev opreme od leta 2016 MITRE CVE pokriva le proizvode, ki so objavljeni na prednostnem seznamu.

Bazo CVE uporablja ameriški US-CERT, ki deluje pod okriljem ameriške vlade in NIST (National Institute of Standards and Technology). Za vsak CVE doda še dodatne informacije in ocene ter jih objavi v bazi NVD (National Vulnerability Database) [78]. NVD baza je vzpostavljena z namenom avtomatizacije upravljanja ranljivosti, merjenja varnosti in preverjanja skladnosti.

Med drugim US-CERT vsaki objavljeni CVE doda CVSS (Common Vulnerability Scoring System), ki numerično opredeli stopnjo tveganja na lestvici 0 do 10, pri čemer 0 pomeni najmanjše tveganje, 10 pa največje tveganje v primeru, da pride do izkoriščanja določene ranljivosti. Način ocenjevanja CVSS lahko bralec najde podrobno obrazložen v [57] in [78]. Danes se uporabljata dve različici tega postopka, in sicer 2.0 in 3.0. Na osnovi te ocene se ranljivost uvrsti v eno od treh skupin tveganj:

a) nizko tveganje – ranljivost dosega oceno od 0.0 do 3.9,
b) srednje tveganje - ranljivost dosega oceno od 4.0 do 6.9,
c) visoko tveganje - ranljivost dosega oceno od 7.0 do 10.0.

Poleg numerične ocene tveganja ocena CVSS doda tudi naslednje informacije:

- Pristopni vektor (angl. access vector) da informacijo, na kakšen način lahko napadalec zlorabi ranljivost. Možne vrednosti so: internet, lokalno omrežje, lokalni dostop.
- Zahtevnost pristopa (angl. access complexity): visoka, srednja, nizka.
- Potreba po avtentikaciji za zlorabo ranljivosti (authentication): brez avtentikacije, posamezna avtentikacija, več instanc.
- Vpliv na zaupnost podatkov (angl. confidentiality impact): brez vpliva, delni, popoln vpliv.

- Vpliv na integriteto podatkov (angl. integrity impact): brez vpliva, delni, popoln vpliv.
- Vpliv na dosegljivost (angl. availability impact): brez vpliva, delni, popoln vpliv (DoS).

Sledi primer XML zapisa za ranljivost CVE-2016-0179.
(vir: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0179)

```
<entry id="CVE-2016-0179">
  <vuln:vulnerable-configuration id="http://nvd.nist.gov/">
   <cpe-lang:logical-test operator="OR" negate="false">
    <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_10:1511"/>
    <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_10"/>
    <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_rt_8.1"/>
    <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2"/>
    <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_8.1"/>
   </cpe-lang:logical-test>
  </vuln:vulnerable-configuration>
  <vuln:vulnerable-software-list>
   <vuln:product>cpe:/o:microsoft:windows_10:1511</vuln:product>
   <vuln:product>cpe:/o:microsoft:windows_8.1</vuln:product>
   <vuln:product>cpe:/o:microsoft:windows_rt_8.1</vuln:product>
   <vuln:product>cpe:/o:microsoft:windows_10</vuln:product>
   <vuln:product>cpe:/o:microsoft:windows_server_2012:r2</vuln:product>
  </vuln:vulnerable-software-list>
  <vuln:cve-id>CVE-2016-0179</vuln:cve-id>
  <vuln:published-datetime>2016-05-10T21:59:18.687-04:00</vuln:published-datetime>
  <vuln:last-modified-datetime>2016-06-09T14:15:46.673-04:00</vuln:last-modified-datetime>
  <vuln:cvss>
   <cvss:base_metrics>
    <cvss:score>9.3</cvss:score>
    <cvss:access-vector>NETWORK</cvss:access-vector>
    <cvss:access-complexity>MEDIUM</cvss:access-complexity>
    <cvss:authentication>NONE</cvss:authentication>
    <cvss:confidentiality-impact>COMPLETE</cvss:confidentiality-impact>
    <cvss:integrity-impact>COMPLETE</cvss:integrity-impact>
    <cvss:availability-impact>COMPLETE</cvss:availability-impact>
    <cvss:source>http://nvd.nist.gov</cvss:source>
    <cvss:generated-on-datetime>2016-06-09T12:44:41.330-04:00</cvss:generated-on-
datetime>
   </cvss:base_metrics>
  </vuln:cvss>
  <vuln:cwe id="CWE-284"/>
  <vuln:references xml:lang="en" reference_type="VENDOR_ADVISORY">
   <vuln:source>MS</vuln:source>
   <vuln:reference href="http://technet.microsoft.com/security/bulletin/MS16-057"
xml:lang="en">MS16-057</vuln:reference>
  </vuln:references>
  <vuln:references xml:lang="en" reference_type="UNKNOWN">
   <vuln:source>SECTRACK</vuln:source>
   <vuln:reference href="http://www.securitytracker.com/id/1035825"
xml:lang="en">1035825</vuln:reference>
  </vuln:references>
  <vuln:summary>Windows Shell in Microsoft Windows 8.1, Windows Server 2012 R2, Windows
RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a
crafted web site, aka "Windows Shell Remote Code Execution Vulnerability."</vuln:summary>
```

```
</entry>
```

Slika 21: Primer XML zapisa za CVE-2016-0179 (vir: NVD CVE)

Iz slike 21 razberemo, da gre za resno ranljivost v operacijskih sistemih Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, in Windows 10, ki ima lahko velik vpliv na zaupnost in integriteto podatkov ter na delovanje sistema.

NIST poleg baze NVD CVE vzdržuje še naslednje baze z namenom lažje avtomatizacije, korelacije in enolične identifikacije proizvodov in virov ranljivosti:

1) CPE (Common Platform Enumeration) je baza, ki vsebuje strukturno poimenovane sheme za operacijske sisteme, platforme, programske pakete (proizvode) ter proizvajalce z namenom zagotavljanja enolične identifikacije (ranljive) programske kode. CPE struktura je sledeča:

   cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}

   Če je del definicije CPE prazen (::, :*:, :-:, …), to pomeni poljubno vrednost.

   Pomemben in obvezen je predvsem prvi del CPE "cpe:/{part}:{vendor}:{product}".

   Pri tem ima {part} naslednje kodiranje:

part	naziv
o	operacijski sistem
a	aplikacija
h	strojna oprema (hardware)

Tabela 26: CPE - kodiranje naziva {part}

   S pomočjo te strukture lahko enolično identificiramo programsko ali strojno opremo, ki je izpostavljena posamezni CVE ranljivosti, in se izognemo besednemu opisovanju v obliki “MS Windows 7 sp1, Microsoft Windows 7 x64, in podobno”.

   Primer CPE kode za operacijski sistem Windows 8 x86, ki velja za vse različice in nameščene popravke:
   cpe:/o:microsoft:windows_8:-:-:x86

   Primer CPE kode za brskalnik Mozilla Firefox 45.0.2
   cpe:/a:mozilla:firefox:45.0.2

2) CWE (Common Weakness Enumeration) [68] zagotavlja enovito zbirko splošno znanih opisov za napake, storjene v izvorni programski kodi, dizajnu ali sistemski arhitekturi. Te napake namreč na koncu pripeljejo do ranljivosti, ki jih obravnava CVE. Na ta način je možno podobno kot s CPE enolično določiti, kateri CWE so vzrok za ranljivost.

Primer na sliki 21 nam sporoča, da gre za CWE-284, ki pomeni naslednje: "Programska oprema ne omejuje dostopa ali nepravilno omejuje dostop do virov nepooblaščenemu akterju."
(vir: http://cwe.mitre.org/data/definitions/284.html)

3) CAPEC (Common Attack Pattern and Classification) [63] je slovar in klasifikacijska taksonomija znanih napadov, ki jih lahko pri svojem delu uporabijo analitiki, razvijalci, testerji in predavatelji ter s tem povečajo razumevanje o napadih in izboljšajo obrambo sistemov IKT.

4) SCAP (Security Content Automation Protocol) [95] je zbirka interoperabilnih specifikacij (CVE, CCE, CPE, CVSS, XCCDF, OVAL), zbranih na predlogih skupnosti. Cilj NIST-a je višji kot samo upravljanje z ranljivostmi. Mnogi varnostni postopki in rešitve si lahko pomagajo s standardiziranimi izrazi in poročili. Vizija je nadaljnja ekspanzija na področje skladnosti (compliance), sanacije in omrežnega nadzora za povečanje varnosti.

5.2 Metodologije analiz podatkov baze CVE

Prek spletnih medijev lahko najdemo mnogo analiz ranljivosti na osnovi baze CVE. Večinoma poskušajo z analizo pojavljanja določenih ključnih besed v opisu (angl. summary) prešteti, kolikokrat se pojavi določena programska oprema ali operacijski sistem, ter na podlagi tega sklepati, kateri programi ali operacijski sistemi so najbolj ranljivi. Navadno štejejo ranljivosti, v katerih nastopa proizvod ali storitev. V praksi se uporabljajo razni načini avtomatizacije teh postopkov, saj je ročno praktično nemogoče obdelovati 76.311 CVE zapisov ranljivosti, ki so nastali od leta 2002 do junija 2016.

Stephan Neuhaus in Thomas Zimmermann [10] sta izdelala neodvisen pristop k določanju trendov ranljivosti. Pri tem se nista opirala na CPE ali CWE oziroma kakšen drug klasifikacijski sistem, temveč sta uporabila latentno Dirichletovo alokacijo (LDA), nenadzorovano tehniko učenja na besedah v opisu. S tem sta prišla do svojega klasifikacijskega sistema, imenovanega »model tematik«. Ta model poleg prepoznavanja pogostih tematik omogoča avtomatiziran način za prepoznavo nastajajočih trendov. Prav ta tehnika je omogočila, da sta napovedala trend nove veje ranljivosti v aplikacijskih strežnikih, o katerem v letu 2009, ko je nastal članek, še ni bilo veliko govora. Od 2002 do 2008 so te ranljivosti zrasle le za 20.6%, od leta 2008 do 2009 pa kar za 83.2%.

Minzhe Guo in Ju An Wang [4] pa sta s pomočjo CVE, CPE, CWE, CAPEC ustvarila koncept strojno razumljivega semantičnega zapisa, ki je pomemben korak k dejanski uporabi SCAP-a v praksi. Kot primer sta razvila rešitev "Software Vulnerability Protege", ki med drugim zna na podlagi strojnih semantičnih pravil poiskati podobne ranljivosti za določeno CVE ranljivost.

Opisana primera in podobne metode so zelo uporabni pristopi za ugotavljanje statističnih ranljivosti po proizvodih in časovnih obdobjih, ne pa tako zelo v vsakodnevnem življenju, saj imamo v praksi običajno nameščeno točno določeno programsko opremo, ki ima točno določeno verzijo in servisni popravek. Na

primer: »Windows 10 x64 sp1« ali »Mozilla Firefox 41.0.0«. Pri tem pa se pojavi vprašanje, ali bomo naš sistem pravilno ocenili, če gledamo splošne ranljivosti za ta proizvod. Prav zato sem za namen nadaljnjih analiz v tem delu ustvaril orodje CVE-analyzer (priloga 1), ki na osnovi točno določenega nabora programov vrne število in težo ranljivosti ter omogoča enostavno kopičenje dodatnih informacij CVSS (CVSS: score, access vector, availability impact ipd.).

5.3 Uporaba odprtokodne programske opreme v slovenskih podjetjih

Na vprašanje, ali so slovenska podjetja bolj ranljiva zaradi uporabe odprtokodne programske opreme, ni možno dati enostavnega odgovora. Ne poznamo namreč različic in kombinacij naložene programske opreme, niti ali je šlo za odprtokodno, licenčno ali le za kombinacijo programske opreme. Prav tako ne moremo vedeti, ali je bila ta programska oprema pravilno nastavljena in vzdrževana ali pa samo nameščena (out-of-the-box) ter pozabljena. Ne vemo, kako kakovostna (kompleksna) gesla so bila v uporabi in podobno.

Da bi prikazali postopek takšnega ocenjevanja, se bomo najprej seznanili z bazo ranljivosti CVE, potem pa naredili analizo realnega primera z uporabo licenčne in odprtokodne programske opreme. Na tem primeru bomo po ponovljivi metodi ugotovili, kateri sistem je tehnično gledano bolj varen. Potem bomo metodo posplošili in poskušali podati splošno oceno ter odgovor na hipotez H3 in H4.

5.4 Postopek določanja programske opreme za analizo

V nadaljevanju bom prikazal, kakšen bi lahko bil postopek merjenja ranljivosti programske opreme nekega računalniškega sistema, ki bi ga izvedlo podjetje, če bi želelo zmanjšati ranljivost svojih IS. To je drugačen pristop, kot če bi gledali zgolj ocene na osnovi statističnih podatkov. Na ta način želim najti pravila, ki bi omogočala ne le zaznavanje stopnje ranljivosti, temveč tudi nudila pomoč odločevalcem pri izbiri primerne programske opreme, ki bi v prihodnje imela čim manj ranljivosti. Te žal v času odločanja niso vedno znane, poskusil pa bom najti pravila za določanje na osnovi preteklih trendov.

Strežniki in delovne postaje se nameščajo na osnovi potreb, ki jih morajo opravljati. Za delitev na strežnik ter delovno postajo sem se odločil zato, ker navadno na strežnike ne nameščamo pisarniške programske opreme, brskalnikov, avdio/video multimedijskih predvajalnikov, pregledovalnikov e-pošte in podobno. Prav tako velja obratno, torej da na delovne postaje ne nameščamo strežnikov za e-pošto, javnih spletnih strežnikov, strežnikov za podatkovne baze in podobno. Takšna postavitev je lahko zato tudi modularna, kar pomeni, da lahko uporabljamo povsem licenčni strežnik, v pisarni pa delovne postaje na popolni odprtokodni osnovi. Shema in poimenovanje sledi v tabeli 27.

	ODPRTOKODNI	LICENČNI
Strežnik	OST	LST
Delovna postaja	ODP	LDP

Tabela 27: Model primerjave licenčne ter odprtokodne programske opreme

Zaradi množice možnih konfiguracij (nastavitev) sistemov v podjetjih je primerjava izpostavljenosti podjetja zelo težka. Na primer: v podjetju imajo lahko 200 računalnikov in 10 strežnikov, od tega pa je na primer spletni strežnik nameščen na treh strežnikih. Za poenostavitev bom pripravil navidezno[13] namestitev dveh strežnikov in dveh delovnih postaj. Pri tem bom v enem primeru uporabil le odprtokodno programsko opremo, v drugem primeru pa licenčno programsko opremo. Izhajam iz predpostavke, da z izbrano programsko opremo podjetje in zaposleni lahko izvedejo iste naloge. Te naloge (poenostavljeno gledano) so naslednje.

Strežnik mora zagotavljati:

- poslovno e-pošto za vse zaposlene,
- predstavitvene spletne strani podjetja z možnostjo spletne trgovine.

Delovna postaja mora zaposlenemu zagotavljati:

- upravljanje z elektronsko pošto,
- delo z dokumenti, preglednicami in predstavitvenimi datotekami,
- brskanje po svetovnem spletu,
- osnovno urejanje slik in fotografij,
- prikaz multimedijskih vsebin (oglasne pasice, filmi, videoposnetki),
- protivirusno zaščito.

Pri izboru programske opreme za strežnik se bomo zaradi možnosti lažjih nadaljnjih primerjav z že predstavljenimi analizami posledic incidentov v poglavju 4.2 postavili v leto 2010[14]. Seveda pa je postopek enostavno mogoče postaviti v katerokoli obdobje (vključno z današnjim dnem), ki je pokrito v CVE in imamo za to obdobje dovolj dobre podatke o najpogosteje uporabljeni programski opremi. V primeru, da sami izbiramo, katero programsko opremo bomo izbrali, pa je postopek še enostavnejši.

[13] Podatki SURS o uporabljeni PO ne podajo dovolj podrobnih informacij o uporabi PO v slovenskih podjetjih.

[14] Programska oprema za analizo (zlasti oznaka različice) je bila izbrana na osnovi pregledovanja spletnih virov z informacijami o izidu navedene PO. Upoštevane so bile različice z izidom konec leta 2009 ali v prvem mesecu 2010.

	ODPRTOKODNA PO	LICENČNA PO
Operacijski sistem	Linux (Debian, Ubuntu, CentOS...), FreeBSD, SuSe	Microsoft Windows XP/Vista/7 Microsoft Windows Server 2003/2008/ 2008 R2
Spletni brskalnik	Mozilla FireFox, Google Chrome	Internet Explorer
Pisarniška prog. oprema	Open Office / Libre Office Mozilla Thunderbird VLC Player, GomPlayer, BS Player, 7-Zip	Microsoft Office MS Outlook Windows Media Player WinZip, WinRar
Programi za delo s slikami	GIMP	Adobe Photoshop
Spletni strežniki	Apache Server	Microsoft IIS 5.1-6.0
Programska oprema na strežniku	PHP	Asp.Net, MS .Net Framework
Podatkovne baze	MySQL, Postgre SQL, Firebird	MS SQL, Oracle
Strežniki za e-pošto	Sendmail, Postfix	Microsoft Exchange Server 2003
Protivirusne rešitve	ClamAV	Symantec Antivirus, AVG Free, Avast
Razvojna orodja	ECLIPSE	Microsoft Visual Studio
Ostalo	Sun Java JRE 1.6.x[15] Adobe Flash Player 10.x[16]	Sun Java JRE 1.6.x Adobe Flash Player 10.x

Tabela 28: Kategorije dostopne programske opreme (odprtokodni, licenčni model) v letu 2010

STREŽNIK	ODPRTOKODNI (OST)	LICENČNI (LST)
Operacijski sistem	Cent OS 5.4 x64 (Linux kernel 2.6.18.1)	Windows Server 2003 sp2 x64
Spletni strežnik	Apache server 2.2.3	MS IIS 6.0
Programski jezik	PHP 5.1.6	Asp.Net (2.0 sp2, 3.5 sp1)
Podatkovna baza	MySQL 5.0.77	MS SQL Server 2008
Strežnik za e-pošto	Exim 4.63 + Dovecot (1.2.0)	Microsoft Exchange Server 2007 p2 x64

Tabela 29: Izbor programske opreme za strežnik (ST), leto 2010

V letu 2010 je 47% spletnih strani teklo na spletnem strežniku MS IIS 6.0, na Apache-ju pa 23.40% zato sem se odločil izbrati ta dva spletna strežnika [81].

[15] Sun Java ni odprtokodni proizvod, vendar je navadno nameščen tako na licenčnih operacijskih sistemih (MS Windows) kot tudi na odprtokodnih sistemih (Linux). Uporablja se za zaganjanje aplikacij, napisanih v Javi.

[16] Adobe Flash ni odprtokodni proizvod, vendar je navadno nameščen tako na licenčnih operacijskih sistemih (MS Windows) kot tudi na odprtokodnih sistemih (Linux). Uporablja se za multimedijo v brskalniku (flash oglasi, igre, ipd.).

DELOVNA POSTAJA	ODPRTOKODNI (O)	LICENČNI (L)
Operacijski sistem	Cent OS 5.4 (32-bit) (Linux kernel 2.6.18.1)	Windows XP Professional sp3 (32-bit)
Spletni brskalnik	Mozilla Firefox 3.5.6	Internet Explorer 8
Program za e-pošto	Mozilla Thunderbird 3.0	MS Outlook 2007 sp2
Pisarniška programska oprema	Open Office 3.1.1	MS Office 2007 sp2
PDF pregledovalnik	Evince 0.6	Adobe Acrobat Reader 9.0
Multimedia	VLC Media Player 1.0.3	Windows Media Player 11
	Adobe Flash Player (10.0.12.36)	Adobe Flash Player (10.0.12.36)
Programi za delo s slikami	GIMP 2.6.11	Adobe Photoshop CS4 (v11)

Tabela 30: Izbor programske opreme za delovno postajo (DP), leto 2010

Na osnovi analize uporabljene programske opreme s pomočjo podatkov v bazi CVE bom skušal ugotoviti ranljivost posameznega sistema v letu 2010. Pri tem predpostavljam, da v podjetju niso dali poudarka nadgradnjam in varnostnim posodobitvam sistema v tem letu.

Za avtomatsko reševanje problema sem se na podlagi pregleda virov ter pristopov opisanih v predhodnih poglavjih odločil, da je najbolje napisati svojo programsko opremo, ki bo dala odgovore na ta vprašanja. V ta namen je nastalo ogrodje CVE-analyzer, ki je podrobneje opisano v prilogi tega dela. Priložena je tudi polna izvorna koda in predloge za analize v nadaljevanju.

5.5 Analiza uporabljene PO s CVE-analyzerjem

Postopek analize je bil sledeč. Najprej sem na podlagi izbrane programske opreme [29, 30] poiskal pripadajoče klasifikatorje CPE. Pri tem sem si pomagal z lastno podatkovno tabelo uvoženih nvdcve-2.0-{LETO}.xml ranljivosti ter official-cpe-dictionary_v2.3.xml [78]. Te sem uporabil za pripravo štirih naborov konfiguracij sistemov za CVE-analyzer, kot sledi iz gornjih tabel. V naslednjem koraku sem zagnal paketno obdelavo in počakal na CSV izpise.

V tabeli 31 vidimo oceno ranljivosti za izbrani odprtokodni spletni strežnik z upoštevanimi vsemi znanimi ranljivostmi do vključno konca leta 2010. Skupno analiza najde 344 ranljivosti s skupno težo 1.918,5 točk CVSS. Od tega ima 147 ranljivosti, ki omgočajo napad preko oddaljenega omrežja. V operacijskem sistemu z jedrom Linux Kernel 2.6.18 x64 je CVE-analyzer našel 155 ranljivosti, ki lahko privedejo do popolne neodzivnosti sistema.

V tabeli 32 vidimo oceno ranljivosti za izbrani licenčni strežnik z upoštevanimi vsemi znanimi ranljivostmi do vključno konca leta 2010. Skupno ima 197 ranljivosti s skupno težo 1.525,8 CVSS točk. Od tega ima 156 ranljivosti, ki omočajo napad preko oddaljenega omrežja (interneta). V operacijskem sistemu je 123 ranljivosti, ki lahko privedejo do popolne neodzivnosti sistema.

Izračun relativne razlike med dvema vrednostma

Za lažjo primerjavo med številčnimi vrednostmi bom v nadaljevanju uporabil formulo (5.1) za izračun relativne razlike med dvema vrednostma. Formula se uporablja, kadar želimo narediti primerjavo dveh eksperimentalnih vrednosti, od katerih nobene ne moremo smatrati za "pravo" vrednost. Vrednost razlike v procentih se izračuna kot absolutna razlika vrednosti, deljena z aritmetično sredino absolutnih vrednosti spremenljivk, pomnoženo s 100 [55], [82].

$$d_r(x,y) = \frac{|x-y|}{\left(\frac{|x|+|y|}{2}\right)} \cdot 100 \qquad (5.1)$$

Proizvod	Število ranljivosti	Točke CVSS (vsota)	Točke CVSS (povprečje)	Pristopni vektor: OMREŽJE	Vpliv na razpoložljivost sistema: POPOLN
Linux Kernel 2.6.18 x64	225	1.204,20	5,35	46	155
Apache server 2.2.3	26	133,6	5,14	22	6
PHP 5.1.6	74	474,8	6,42	65	11
MySQL 5.0.77	8	46,4	5,8	7	1
Exim 4.63 + Dovecot 1.2.0	11	59,5	5,41	7	2
Vsota:	**344**	**1.918,5**		147	175

Tabela 31: Ocena ranljivosti za odprtokodni strežnik (OST), do konca leta 2010

Proizvod	Število ranljivosti	Točke CVSS (vsota)	Točke CVSS (povpr.)	Pristopni vektor: OMREŽJE	Vpliv na razpoložljivost sistema: POPOLN
Windows Server 2003 sp2 x64	138	1.114,60	8,08	97	123
MS IIS 6.0	17	107,7	6,34	17	5
Asp.Net (2.0, 3.5)	26	174,4	6,71	26	11
MS SQL Server 2008	11	102,3	9,3	11	11
Microsoft Exchange Server 2007 sp2 x64	5	26,8	5,36	5	0
Vsota:	**197**	**1.525,8**		156	150

Tabela 32: Ocena ranljivosti za izbrani licenčni strežnik (LST), do konca leta 2010

Predpostavimo, da v organizaciji uporabljamo LST (tabela 32) in nas zanima, ocena varnosti, če preidemo na OST (tabela 31).

Število ranljivosti LST = 197. Teža ranljivosti LST = 1.525,8 točk CVSS.
Število ranljivosti OST = 344. Teža ranljivosti OST = 1.918,5 točk CVSS.

Ocena prehoda na OST strežnik:

(5.2)

$$d_r(\text{stRanljivosti\_OST; stRanljivosti\_LST}) = \frac{|344-197|}{\left(\frac{|344|+|197|}{2}\right)} \cdot 100 = \frac{147}{270{,}5} \cdot 100 = 54{,}3\%$$

$$d_r(\text{stTockCVSS\_OST; stTockCVSS\_LST}) = d_r(1525{,}8;\ 1918{,}5) = 22{,}8\% \qquad (5.3)$$

Iz opisanega primera sklepamo, da je izbrani odprtokodni strežnik (LST) s 54,3% večjim številom ranljivosti (5.2) tudi po teži ranljivosti za 22,8% bolj ranljiv kot licenčni strežnik (5.3). Na podlagi ocene ranljivosti se pri takšnem naboru programske opreme najverjetneje ne bomo odločili za prehod na OST.

Analiza ranljivosti delovne postaje je vrnila rezultate v tabelah 33 in 34.

Proizvod	Število ranljivosti	Točke CVSS (vsota)	Točke CVSS (povpr.)	Pristopni vektor: OMREŽJE	Vpliv na razpoložljivost sistema: POPOLN
CentOS 5.4 (Linux Kernel 2.6.18 x32)	226	1.211,10	5,36	46	156
Mozilla Firefox 3.5.x	136	691,4	7,52	90	55
Mozilla Thunderbird 3.0	55	432,9	7,87	53	38
Open Office 3.1.1	8	74,4	9,3	8	8
Evince 0.6	0	0	0	0	0
VLC Media Player 1.0.3	2	14,3	7,15	2	1
Adobe Flash Player for Linux (10.0.12.36)[17]	7	55,4	7,91	6	5
GIMP 2.6.x	2	18,6	9,3	2	2
Vsota:	**435**	**2.838,6**		250	290

Tabela 33: Ocena ranljivosti za izbrano odprtokodno delovno postajo (ODP1), do konca leta 2010

[17] Adobe Flash Player for Linux – gre za licenčno PO, ki je prevedena za delovanje na Unix/Linux sistemih. Zaradi drugačnega delovanja operacijskega sistema ter uporabljenih programskih knjižnic iz baze CVE sledi, da ima bistveno manj ranljivosti kot različica iste verzije za sisteme MS Windows.

Proizvod	Število ranljivosti	Točke CVSS (vsota)	Točke CVSS (povpr.)	Pristopni vektor: OMREŽJE	Vpliv na razpoložljivost sistema: POPOLN
Windows XP Professional sp3 (32-bit)	245	2.008,90	8,2	187	217
Internet Explorer 8	75	537,50	7,17	75	41
MS Outlook 2007 sp2	3	25,4	8,47	3	2
MS Office 2007 sp2	53	472,7	8,92	53	49
Adobe Acrobat Reader 9.0	89	782	8,79	88	78
Windows Media Player 11	13	86	6,62	13	6
Adobe Flash Player (10.0.12.36)	81	695,7	8,59	80	68
Adobe Photoshop CS4 v11	2	18,6	9,3	2	2
Vsota:	561	4.626,8		501	463

Tabela 34: Ocena ranljivosti za izbrano licenčno delovno postajo (LDP1), do konca leta 2010

$$d_r(\text{stRanljivosti\_ODP1}; \text{stRanljivosti\_LDP1}) = d_r(435; 561) = 25\% \quad (5.4)$$

$$d_r(\text{stTockCVSS\_ODP1}; \text{stTockCVSS\_LDP1}) = d_r(2.838,6;\ 4.626,8) = 48\% \quad (5.5)$$

Izračun kaže, da ima licenčna delovna postaja (LDP1) za 25% večje število ranljivosti (5.4) s skupno težo CVSS, ki je 48% večja od teže ranljivosti v ODP1 (5.5).

Vidimo, da največ doprinesejo ranljivosti v Adobe Flash Playerju ter Adobe Acrobat Readerju. Če iz obeh sistemov odstranimo PDF pregledovalnik in Adobe Flash Player, se slika spremeni (tabela 35).

$$d_r(\text{stRanljivosti\_LDP2}; \text{stRanljivosti\_ODP2}) = d_r(391; 429) = 9\% \quad (5.6)$$

$$d_r(\text{stTockCVSS\_LDP2}; \text{stTockCVSS\_ODP2}) = d_r(3.149,1; 2.442,7) = 25\% \quad (5.7)$$

V tem primeru ima LDP2 (tabela 38) manj ranljivosti od ODP2. V odstotkih to predstavlja 9% razliko (5.6). Skupna teža ranljivosti v točkah CVSS sicer še vedno pretehta v prid ODP2 (za 25%, enačba 5.7), vendar analiza že kaže na to, kako pomemben je izbor kombinacije programske opreme.

Licenčni model (LDP2)			Odprtokodni model (ODP2)		
Proizvod	**Št. ranlj.**	**Točke CVSS (vsota)**	**Proizvod**	**Št. ranlj.**	**Točke CVSS (vsota)**
Windows XP Professional sp3 (32-bit)	245	2.008,90	CentOS 5.4 (Linux Kernel 2.6.18 x64)	226	1.211,10
Internet Explorer 8	75	537,5	Mozilla Firefox 3.5.x	136	691,4
MS Outlook 2007 sp2	3	25,4	Mozilla Thunderbird 3.0	55	432,9
MS Office 2007 sp2	53	472,7	Open Office 3.1.1	8	74,4
Adobe Acrobat Reader 9.0	-	-	Evince 0.6	-	-
Windows Media Player 11	13	86	VLC Media Player 1.0.3	2	14,3
Adobe Flash Player (10.0.12.36)	-	-	Adobe Flash Player for Linux (10.0.12.36)*	-	-
Adobe Photoshop CS4 v11	2	18,6	GIMP 2.6.x	2	18,6
Vsota:	**391**	**3.149,1**		**429**	**2.442,7**

Tabela 35: Primerjava licenčne in odprtokodne delovne postaje po številu in teži ranljivosti brez pregledovalnika PDF in Adobe Flash Playerja, do konca leta 2010

Zamenjajmo operacijski sistem "Windows XP Professional sp3" z "Windows 7 Professional (32-bit)". Ta je imel do konca leta 2010 le 92 znanih ranljivosti. Rezultat je viden v tabeli 36.

$$d_r(\text{stRanljivosti\_LDP3};\text{stRanljivosti\_ODP3}) = d_r(238;429) = 57\% \quad (5.8)$$

$$d_r(\text{stTockCVSS\_LDP3};\text{stTockCVSS\_ODP3}) = d_r(1.882,5;2.442,7) = 26\% \quad (5.9)$$

Kot pokaže analiza, je v zadnjem primeru (tabela 36) varnejši licenčni model delovne postaje. Enačbi (5.8, 5.9) pokažeta, da je po številu ranljivosti v tem izboru programske opreme LDP3 za 57% varnejša od ODP3, po teži ranljivosti pa je LDP3 varnejša za 26% glede na ODP3.

Ali lahko torej trdimo, da je v splošnem licenčni model PO varnejši od odprtokodnega? Da in ne. Kot smo videli na osnovi analize, na varnost modela PO pomembno vpliva tudi kombinacija uporabljene PO in seveda tudi dejstvo, ali je bila ta oprema posodobljena na najnovejše različice, ki so navadno varnejše.

Licenčni model (LDP3)			Odprtokodni model (ODP3)		
Proizvod	**Št. ranlj.**	**Točke CVSS (vsota)**	**Proizvod**	**Št. ranlj.**	**Točke CVSS (vsota)**
Windows 7 Professional (32-bit)	92	742,30	CentOS 5.4 (Linux Kernel 2.6.18 x64)	226	1.211,10
Internet Explorer 8	75	537,5	Mozilla Firefox 3.5.x	136	691,4
MS Outlook 2007 sp2	3	25,4	Mozilla Thunderbird 3.0	55	432,9
MS Office 2007 sp2	53	472,7	Open Office 3.1.1	8	74,4
Adobe Acrobat Reader 9.0	-	-	Evince 0.6	-	-
Windows Media Player 11	13	86	VLC Media Player 1.0.3	2	14,3
Adobe Flash Player (10.0.12.36)	-	-	Adobe Flash Player for Linux (10.0.12.36)*	-	-
Adobe Photoshop CS4 v11	2	18,6	GIMP 2.6.x	2	18,6
Vsota:	**238**	**1.882,50**		**429**	**2.442,7**

Tabela 36: Primerjava licenčne in odprtokodne delovne postaje iz tabele (35), uporabljen licenčni operacijski sistem Windows 7

5.6 CVE analiza ranljivosti spletnih brskalnikov

Zanimalo me je ali so slovenska podjetja v letu 2011 bila bolj ali manj ranljiva zaradi uporabe odprtokodnih spletnih brskalnikov. Lahko seveda pogledamo še bolj nazaj v preteklost, tako v CVE bazi kot tudi pri uporabi spletnih brskalnikov, glede na leto izida. Obenem sem pri predmetni analizi upošteval le tri najpogosteje uporabljane brskalnike, ki imajo skupaj več kot 90% delež uporabe.

Da bi poenostavil analizo, sem predpostavljal, da so podjetja skrbno uporabljala zadnje različice spletnih brskalnikov. To pomeni, da so jih posodabljala, ko so bili ti uradno izdani za uporabo v javnosti. Za pomoč pri izdanih različicah brskalnikov po letih sem si pomagal s spletnimi viri za Internet Explorer [73], Mozilla Firefox [71] ter Google Chrome [72].

Analizo sem naredil še za dve leti pred letom 2011 in po njem, da je tako iz dobljenih podatkov lažje izluščiti statistične rezultate kot tudi morebitne trende za odločanje v primerih, ko nimamo na voljo dovolj CVE podatkov za prihodnost.

Predpostavil sem, da podjetje uporablja izključno eno vrsto spletnega brskalnika (Internet Explorer, Mozilla Firefox, Google Chrome). V tabeli so za aktualne različice zapisani tudi meseci izida v obliki (MM/LL), ker bom v formulah za izračun ranljivosti upošteval prejšnjo različico in povprečje ranljivosti v letu 2011, in sicer pod predpostavko, da so uporabniki sproti nadgrajevali različice brskalnikov, ko so bili ti uradno izdani.

Podatki v tabeli 37 so bili zbrani s pomočjo namenskega orodja CVE-analyzer. Pri tem so za vsako CVE-LETO izpisani kumulativni podatki o številu ranljivosti in teži ranljivosti (CVSS SCORE).

Pri številu in teži ranljivosti bom v izračunih upošteval vse do vključno 31.12.2011 objavljene ranljivosti (stolpec CVE-2011). Vse različice brskalnikov, ki bodo zastopane v izračunu, so v tabeli označene odebeljeno. Z modro odebeljeno pisavo pa so označeni licenčni spletni brskalniki.

a) Izračun za Internet Explorer 9. Ker so prve tri mesece uporabniki morali uporabljati še Internet Explorer 8, upoštevam to v formuli, ki se glasi:

Povprečno število ranljivosti brskalnika Internet Explorer v letu 2011:

$$SteviloRanljivosti(IE) = SteviloRanljivosti(IE8)\cdot\frac{3}{12} + SteviloRanljivosti(IE9)\cdot\frac{9}{12}$$

$$SteviloRanljivosti(IE) = 15\cdot\frac{3}{12} + 9\cdot\frac{9}{12} = 13 \qquad (5.10)$$

Povprečna teža ranljivosti brskalnika Internet Explorer v letu 2011:

$$TezaRanljivosti(IE) = TezaRanljivosti(IE8)\cdot\frac{3}{12} + TezaRanljivosti(IE9)\cdot\frac{9}{12}$$

$$TezaRanljivosti(IE) = 340{,}2\cdot\frac{3}{12} + 47{,}4\cdot\frac{9}{12} = 321 \qquad (5.11)$$

V povprečju so bili glede na ta izračun uporabniki licenčnega brskalnika Internet Explorer v letu 2011 izpostavljeni 43 ranljivostim s težo 321 točk CVSS.

b) Izračun za Mozilla Firefox. Ker so prve tri mesece uporabniki morali uporabljati še Firefox 3.6, upoštevam to v formuli (5.12). V letu 2011 je bilo šest izidov novih različic tega brskalnika, zato bom upošteval povprečje znanih ranljivosti za te izide do vključno 31.12.2011[18]:

$$SteviloRanljivosti(Firefox) = SteviloRanljivosti(Firefox\_3.6)\cdot\frac{3}{12}$$

$$+ povp(SteviloRanljivosti(izdaje\_Firefox\_2011))\cdot\frac{9}{12}$$

$$SteviloRanljivosti(Firefox) = 66\cdot\frac{3}{12} + \frac{1}{6}\cdot(55+32+32+3+3+3) = 50 \qquad (5.12)^*$$

$$TezaRanljivosti(Firefox) = TezaRanljivosti(Firefox\_3.6)\cdot\frac{3}{12}$$

$$+ povp(TezaRanljivosti(izdaje\_Firefox\_2011))\cdot\frac{9}{12}$$

[18] *V tabeli 37, glej leto izdaje 2011, brskalnik Mozilla Firefox – št. ranljivosti/točke CVSS po izdaji posamezne različice v tem letu.

$$TezaRanljivosti(Firefox) = 269 \cdot \frac{3}{12} + \frac{1}{6}(413{,}4 + 146{,}2 + 62{,}6 + 16{,}6 + 16{,}6 + 14{,}3) \cdot \frac{9}{12} = 150 \quad (5.13)^*$$

V povprečju so bili glede na ta izračun uporabniki brskalnika Firefox v letu 2011 izpostavljeni 60 ranljivostim s težo 450 točk CVSS.

c) Izračun za Google Chrome. Ker so prva dva meseca morali uporabljati še Google Chrome 8, upoštevam to v formuli. V letu 2011 je bilo potem 8 izidov novih različic tega brskalnika, zato bom upošteval kar povprečje znanih ranljivosti za te izide do vključno 31.12.2011[19]:

$$SteviloRanljivosti(Chrome) = SteviloRanljivosti(Chrome\_8) \cdot \frac{2}{12} + povp(SteviloRanljivosti(izdaje\_Chrome\_2011)) \cdot \frac{10}{12}$$

$$SteviloRanljivosti(Chrome) = 174 \cdot \frac{2}{12} + \frac{1}{8}(241 + 108 + 76 + 43 + 21 + 10 + 12 + 6) \cdot \frac{10}{12} = 53 \quad (5.14)^{**}$$

$$TezaRanljivosti(Chrome) = TezaRanljivosti(Chrome\_8) \cdot \frac{2}{12} + povp(TezaRanljivosti(izdaje\_Chrome\_2011)) \cdot \frac{10}{12} \quad (5.15)^{**}$$

$$TezaRanljivosti(Chrome) = 887{,}3 \cdot \frac{2}{12} + \frac{1}{8}(1633{,}2 + 394{,}9 + 171{,}3 + 152{,}9 + 108{,}6 + 132{,}4 + 175{,}6 + 101{,}1) \cdot \frac{10}{12} = 1.031$$

V povprečju so bili glede na ta izračun uporabniki brskalnika Google Chrome v letu 2011 izpostavljeni 153 ranljivostim s težo 1.031 točk CVSS.

[19] **V tabeli 37, glej leto izdaje 2011, brskalnik Google Chrome – št. ranljivosti/točke CVSS po izdaji posamezne različice v tem letu.

		CVE-2009		CVE-2010		CVE-2011		CVE-2012	
Leto izida	**Brskalnik**	Št. ranljivosti	Točke CVSS (vsota)	Št. ranljivosti	Točke CVSS (vsota)	Št. ranljivosti	Točke CVSS (vsota)	Št. ranljivosti	Točke CVSS (vsota)
2004	Internet Explorer 6	433	2.954,20	475	3.264,50	510	3.514,50	531	3.689,60
	Mozilla Firefox 1.0	216	1.429,50	263	1.782,00	307	2.136,70	403	2.952,80
2005	Internet Explorer 7	161	1.190,90	197	1.460,40	229	1.699,20	253	1.890,50
	Mozilla Firefox 1.5	224	1.514,10	271	1.866,60	314	2.216,30	410	3.032,40
	Mozilla Firefox 2.0	233	1.560,70	280	1.913,20	325	2.272,20	430	3.160,10
2008	**Internet Explorer 8**	34	231,5	75	537,5	**115**	**840,2**	**142**	**1.061,10**
	Mozilla Firefox 3.0	147	1.039,60	205	1.465,10	252	1.833,40	358	2.725,60
	Google Chrome 0.2.149	30	196	129	970,8	386	2.749,50	481	3.423,30
	Google Chrome 0.3.154	23	155,9	122	930,7	379	2.709,40	474	3.383,20
	Google Chrome 0.4.154	23	155,9	122	930,7	379	2.709,40	474	3.383,20
	Google Chrome 1.0.154	28	185,6	163	1.239,60	420	3.018,30	515	3.692,10
2009	Mozilla Firefox 3.5	51	396,1	136	1.031,90	191	1.480,20	296	2.368,10
	Google Chrome 2.0.172	14	99,4	147	1.144,10	404	2.922,80	499	3.596,60
	Google Chrome 3.0.195	5	37,2	138	1.081,90	395	2.860,60	490	3.534,40
2010	**Mozilla Firefox 3.6**	6	26,5	96	696,4	**166**	**1.269,00**	271	2.156,90
	Google Chrome 4.0.249			131	1.022,90	389	2.805,10	484	3.478,90
	Google Chrome 4.1.249			113	916,9	371	2.699,10	466	3.372,90
	Google Chrome 5.0.375			93	768,3	349	2.541,20	444	3.215,00
	Google Chrome 6.0.472			43	343,6	299	2.116,50	394	2.790,30
	Google Chrome 7.0.517			29	223,5	285	1.996,40	380	2.670,20
	Google Chrome 8.0.552			18	114,4	**274**	**1.887,30**	369	2.561,10
2011	**Internet Explorer 9 (03/11)**					**19**	**147,4**	**54**	**437,7**
	Internet Explorer 10							4	33,7
	Mozilla Firefox 4.0 (03/11)*			3	21,6	**55**	**413,4**	211	1.655,00
	Mozilla Firefox 5.0 (06/11)*					**32**	**246,2**	188	1.487,80
	Mozilla Firefox 6.0 (08/11)*					**22**	**162,6**	178	1.404,20
	Mozilla Firefox 7.0 (10/11)*					**13**	**96,6**	168	1.333,20
	Mozilla Firefox 8.0 (11/11)*					**13**	**96,6**	161	1.280,90
	Mozilla Firefox 9.0 (12/11)*					**6**	**44,3**	154	1.229,10
	Google Chrome 9.0.597 (02/11)**					**241**	**1.633,20**	336	2.307,00
	Google Chrome 10.0.648 (03/11)**					**208**	**1.394,90**	303	2.068,70
	Google Chrome 11.0.696 (05/11)**					**176**	**1.171,30**	271	1.845,10
	Google Chrome 12.0.742 (06/11)**					**143**	**952,9**	238	1.626,70
	Google Chrome 13.0.782 (08/11)**					**121**	**808,6**	216	1.482,40
	Google Chrome 14.0.835 (09/11)**					**80**	**532,4**	175	1.206,20
	Google Chrome 15.0.874 (11/11)**					**42**	**275,6**	137	949,4
	Google Chrome 16.0.912 (12/11)**					**16**	**101,1**	111	774,9

Tabela 37: CVE analiza ranljivosti spletnih brskalnikov v letih 2009-2012

V tabeli 38 je zbrano število ranljivosti in teža ranljivosti za brskalnike v letu 2011. To so rezultati enačb od (5.9) do (5.14).

Vrsta brskalnika	Število ranljivosti	Število točk CVSS
MS Internet Explorer	43	321
Mozilla Firefox	60	450
Google Chrome	153	1.031

Tabela 38: Ocena povprečne ranljivosti brskalnikov v letu 2011

d) Analiza glede povprečni na tržni delež brskalnikov v letu 2011.

V letu 2011 je bil v svetovnem merilu povprečni tržni delež brskalnikov naslednji [62]:

- Mozilla Firefox: 41%;
- Google Chrome: 29%;
- Internet Explorer: 24%.

Iz tega dobim razmerje Mozilla Firefox : Google Chrome = 59% : 41%.

Nato preverim povprečno število ranljivosti pri uporabi odprtokodnih brskalnikov (OB). Pri izračunu bom uporabil vrednosti v tabeli 38.

$$StRanljivosti(OB) = StRanljivosti(Firefox) \cdot 0{,}59 + StRanljivosti(Chrome) \cdot 0{,}41$$

$$StRanljivosti(OB) = 50 \cdot 0{,}59 + 53 \cdot 0{,}41 = 99 \quad (5.16)$$

$$TezaRanljivosti(OB) = TezaRanljivosti(Firefox) \cdot 0{,}59 + TezaRanljivosti(Chrome) \cdot 0{,}41$$

$$TezaRanljivosti(OB) = 450 \cdot 0{,}59 + 031 \cdot 0{,}41 = 689 \quad (5.17)$$

Povprečno število ranljivosti OB v letu 2011 je bilo 99.
Povprečna teža ranljivosti OB v letu 2011 je bila 689 točk CVSS.

V tabeli 18 iz statističnih podatkov vidimo, da v povprečju 64% slovenskih podjetij uporablja odprtokodni spletni brskalnik (Mozilla Firefox ali Google Chrome). Predpostavimo, da preostalih 36% podjetij uporablja licenčni brskalnik Microsoft Internet Explorer (LB).

Povprečna izpostavljenost slovenskih podjetij je torej:

$$StRanljivosti(OB, LB) = StRanljivosti(OB) \cdot 0{,}64 + StRanljivosti(LB) \cdot 0{,}36 \quad (5.18)$$

$$StRanljivosti(OB, LB) = 99 \cdot 0{,}64 + 43 \cdot 0{,}36 = 79$$

$$TezaRanljivosti(OB, LB) = TezaRanljivosti(OB) \cdot 0{,}64 + TezaRanljivosti(LB) \cdot 0{,}36$$

$$TezaRanljivosti(OB, LB) = 689 \cdot 0{,}64 + 321 \cdot 0{,}36 = 557 \quad (5.19)$$

Povprečno število ranljivosti spletnih brskalnikov glede na statistične podatke o uporabi in oceni ranljivosti v letu 2011 je bilo 79.

Povprečna teža ranljivosti spletnih brskalnikov glede na statistične podatke o uporabi in oceni teže ranljivosti v letu 2011 je bila 557 točk CVSS.

Za referenco sem vzel LB (Internet Explorer, alineja a) tega poglavja) in preveril, kakšna je ocena izpostavljenosti pri upoštevanju povprečja uporabe OB in LB (alineja d) tega poglavja) v slovenskih podjetjih.

Uporabim že znano formulo za izračun razlike deležev (5.1), kjer uporabim rezultate enačb 5.10 in 5.18.

$$\mathrm{d_r}(\mathrm{stRanljivosti\_OB\_LB};\mathrm{stRanljivosti\_LB}) = d_r(79;\,43) = 59\% \qquad (5.20)$$

Uporabim rezultate enačb 5.11 in 5.19.

$$\mathrm{d_r}(\mathrm{stTockCVSS\_OB\_LB};\,\mathrm{stTockCVSS\_LB}) = d_r(557;321) = 54\% \qquad (5.21)$$

Enačba 5.20 izračuna relativno razliko med povprečnim številom ranljivosti pri uporabi OB in LB, glede na tržne deleže in statistične podatke SURS o uporabi OB v Sloveniji v letu 2011. Ocena pomeni, da so bila podjetja, ki so uporabljala tudi OB, v povprečju izpostavljena 59% večjemu številu ranljivosti kot tista slovenska podjetja, ki so uporabljala izključno LB (Internet Explorer).

Enačba 5.21 izračuna relativno razliko med povprečnim številom točk CVSS ranljivosti pri uporabi OB in LB, glede na tržne deleže in statistične podatke SURS o uporabi OB v Sloveniji v letu 2011. Ocena pomeni, da so bila podjetja, ki so uporabljala tudi OB, v povprečju izpostavljena 54% večjemu številu točk ranljivosti CVSS kot tista slovenska podjetja, ki so uporabljala izključno LB (Internet Explorer). To pomeni, da so imele ranljivosti, vezane na uporabo OB, za slovenska podjetja v letu 2011 povprečno 54% večjo težo, kot če bi podjetja uporabljala izključno LB.

Na osnovi opravljene analize statističnih podatkov o uporabi odprtokodnih spletnih brskalnikov v slovenskih podjetjih v letu 2011 in primerjave rezultatov z analizo podatkov baze NVD CVE za to obdobje, lahko potrdim hipotezo H3 za leto 2011.

H3: Slovenska podjetja, ki uporabljajo odprtokodne spletne brskalnike, so bolj ranljiva od slovenskih podjetij, ki uporabljajo izključno licenčne spletne brskalnike.

Opombe:

1. Pri analizi sem upošteval idealne pogoje, to pomeni, da vsi uporabniki ažurno nadgrajujejo brskalnike takoj, ko so na voljo posodobljene različice. V praksi najbrž to sicer dela le določen odstotek podjetij, kar dejanske rezultate opravljene analize dodatno obrne v prid potrditvi hipoteze H3.
2. V rezultatih točke d) tega poglavja je upoštevana tudi uporaba LB Internet Explorer za 36% podjetij, ki ne uporabljajo OB. To dejansko zniža oceno

ranljivosti (v prid zavrnitvi H3). Če bi upošteval strogo delitev OB, LB, bi še bolj z gotovostjo lahko potrdil H3.

3. Analiza je bila narejena le za leto 2011. Za bolj celovito sliko bi bilo potrebno analizo z uporabo predstavljene metodologije razširiti še v naslednja leta, vse do danes.

Analiza podatkov baze NVD CVE je bila narejena s pomočjo orodja CVE-analyzer, ki sem ga razvil v okviru tega magistrskega dela za namen analiz, opravljenih v tem poglavju. Programski izpisi in izpisi analiz so dostopni na priloženem nosilcu DVD.

Priporočilo za uporabo odprtokodnih brskalnikov
Tabela 37 kaže še en pomemben trend, in sicer, koliko ranljivosti je bilo odkritih v naslednjem letu (CVE-2012). Jasno razvidno je, da ima spletni brskalnik Google Chrome v povprečju dvakrat toliko ranljivosti kot spletni brskalnik Mozilla Firefox, Mozilla Firefox pa od dva do trikrat toliko kot licenčni spletni brskalnik Internet Explorer. Predpostavljam, da ob objavi neke PO, ta že vsebuje ranljivosti, le da te še niso javno znane. Glede na ta dejstva priporočam podjetjem in posameznikom, naj uporabljajo najnovejši Internet Explorer. Če tega ne morejo ali ne želijo, pa naj med odprtokodnimi spletnimi brskalniki namesto brskalnika Google Chrome raje izberejo brsklanik Mozilla Firefox.

5.7 Ocena izpostavljenosti slovenskih podjetij zaradi uporabe odprtokodne programske opreme

V uvodu sem zastavil tudi naslednjo hipotezo.

H4: Če (slovensko) podjetje uporablja odprtokodno programsko opremo, potem je zaradi napak v tej opremi varnostno bolj izpostavljeno kot (slovensko) podjetje, ki uporablja izključno licenčno programsko opremo.

Te hipoteze na osnovi analize v poglavjih 5.5 in 5.6 ne morem ne potrditi ne ovreči. Potrebna je dodatna analiza.

Da bi lahko z večjo gotovostjo potrdil ali zavrnil hipotezo, bi moral vedeti veliko več o tem:

a) kako pogosto podjetja posodabljajo PO;
b) koliko imajo strežnikov ali DP, ki jih zaradi raznih razlogov ne posodabljajo že leta (npr. licence, posebna programska oprema za nadzor proizvodnih linij, ki teče izključno na starih sistemih);
c) kako na druge načine varujejo sisteme iz alineje b);
d) ali redno skrbijo za pregled in testiranje konfiguracij sistemov;
e) v kolikšni meri uporabljajo kombinacijo odprtokodnih in licenčnih programov (samo licenčne, mešano, samo odprtokodne);
f) ali skrbijo, da imajo na strežnikih in DP naloženo izključno PO, ki jo potrebujejo;

g) ali formalno načrtujejo namestitev novih različic ali prehod na druge pakete programske opreme (zaradi licenc, funkcionalnosti, varnosti) ipd.

Obenem bi bilo potrebno narediti podrobne analize in primerjave ranljivosti odprtokodne in licenčne programske opreme, ki se uporablja za podobne namene. Pri tem bi bilo potrebno upoštevati tudi časovna obdobja izida in nadgradenj programske opreme.

Če pa se naslonim na analizo v poglavju 5.6 in pri tem upoštevam, da je v letu 2011 v povprečju 64% podjetij uporabljalo odprtokodni spletni brskalnik in kar 72% podjetij odprtokodno PO, bi lahko, glede na jasen rezultat analize ranljivosti odprtokodnih spletnih brskalnikov v poglavju 5.6 in glede na potrditev hipoteze H3, s pridržkom pritrdil tudi hipotezi H4.

Za gotovo potrditev bi bilo potrebno podobno primerjalno analizo, kot sem jo naredil za spletne brskalnike v poglavju 5.6, narediti še za naslednje načine uporabe programske opreme:
a) uporabo odprtokodnega operacijskega sistema;
b) uporabo odprtokodne pisarniške programske opreme;
c) uporabo odprtokodne programske opreme za spletne strežnike;
d) uporabo odprtokodne programske opreme v podjetjih - strežniki za e-pošto.

Zgolj na podlagi zgoraj navedenega za spletne brskalnike seveda ne moremo posplošeno reči, da je odprtokodna PO manj varna. Da bi to lahko z gotovostjo trdil, bi bilo potrebno zbrati več statističnih podatkov o dejanski vrsti in različicah licenčnih in odprtokodnih operacijskih sistemov ter ostale programske opreme, ki je v uporabi v istem časovnem obdobju, in te podatke primerjati tudi s posledicami nastalih incidentov, tam kjer se uporablja določena oziroma znana programska oprema. Šele tedaj bi lahko naredil bolj gotovo primerjavo ranljivosti in s tem tudi celovite izpostavljenosti slovenskih podjetij ranljivostim.

Ostale ugotovitve
Pri uporabi baze CVE je dobro preveriti anomalije, ki se pojavijo. V postopkih analize sem namreč zasledil najmanj dva CVE zapisa, ki sta verjetno klasificirana v CVE za napačno leto. Ta dva sta:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-7293

Zaradi tega sem CVE-analyzer dodelal tako, da upošteva izključno <vuln:published-datetime>.

5.8 Smernice za formalizacijo in uporabo CVE pri izboru IKT opreme

5.8.1 Formalizacija postopkov z rastjo podjetja

V podjetjih je potrebno z večanjem števila zaposlenih stremeti k formalizaciji in unifikaciji sistemov in postopkov. To pomeni, da zaposleni uporabljajo operacijski sistem enakega tipa, enako pisarniško programsko opremo ter da se na strežnikih

namešča določen tip strežniške programske opreme. To prinaša naslednje prednosti:

1) Enostavnejše upravljanje, konfiguracija sistemov in povezljivost [7].
2) Zaposleni si lažje medsebojno pomagajo pri reševanju težav.
3) Enostavna priprava in posodabljanje navodil za uporabo in prenos znanja.
4) Podporna služba hitreje rešuje morebitne težave, ker pozna programsko opremo. Če se ena težava pojavi na enem mestu in jo uspešno odpravijo, bo odprava na naslednjem mestu veliko enostavnejša, saj že poznajo postopek.
5) Če gre za licenčno programsko opremo, to omogoča lažje predvidevanje stroškov najemov in licenc.
6) Za namestitev novih delovnih postaj ali strežnikov se lahko pripravijo predloge. Te znatno zmanjšajo potreben čas od prejema zahteve za vzpostavitev nove delovne postaje (za novo delovno mesto) ali novega strežnika do dejanske vzpostavitve.

Takšno poenotenje sistemov pa ima tudi slabosti, in sicer:

1) Vezanost na enega proizvajalca programske opreme.
2) Sistemi imajo skupne ranljive točke. Napadalec (heker, računalniški virus ali črv) ima veliko lažje delo, ko je enkrat v omrežju, saj lahko z določeno vrsto napada na odkrito ranljivo točko hitro ogrozi celotno omrežje [7].

5.8.2 Formalizacija postopka izbora predpisane PO s pomočjo analize podatkov CVE

Na osnovi analize in ugotovitev menim, da bi organizacije lahko bolje izkoristile znane metodologije in pristope pri uvajanju ali menjavi programske opreme, in sicer:

1) Na osnovi uporabe predpisane (točno določene) PO in s pomočjo predstavljene analize bi lahko precej dobro predvidele ranljivost posameznih konfiguracij glede na sedanje in pretekle podatke v CVE.
2) Še preden bi se organizacije odločile za nabor programske opreme, ki bi jo vpeljale, bi lahko naredile analizo znanih ranljivosti. Glede na odstotek strežnikov oziroma delovnih postaj v organizaciji bi lahko določile tudi izpostavljenost organizacije glede na izbrano PO. Po potrebi bi tako lahko za določeno PO našle varnejšo alternativo, ki licenčno, vsebinsko in funkcionalno ustreza zamenjani PO.

5.8.3 Vizija varnejše uporabe IKT programske opreme

V današnjem hitro razvijajočem se svetu tehnologije IKT moramo imeti pred očmi možnost avtomatizacije, kjer je to možno. V ta namen bi predlagal organizacijam uporabo oziroma razvoj naslednjih storitev:

1) Programska storitev (angl. agent) – podobno kot protivirusni program (lahko v povezavi s protivirusno rešitvijo), nameščena na OS, ki spremlja naloženo programsko opremo glede na vir in različico (verzijo) ter izvaja preverjanje znanih ranljivosti v bazi CVE. Na osnovi tega nam lahko predlaga posodobitve ali menjavo določene programske opreme in nas opozarja pri tako imenovanih 0-dnevnih (angl. zero-day) ranljivostih. Prednost tega

pristopa je v natančnosti zaznane PO in hitrem opozarjanju, takoj ko je znana nova ranljivost. Slabosti takšne storitve pa so poraba virov na sistemu, možna uvedba novih ranljivosti z dodatno naloženo PO in možen zadržek zaradi zasebnosti oziroma zaupnosti podatkov v sistemu organizacije.

2) Druga možnost je programska storitev, ki preko omrežja naredi popis znane programske in strojne opreme ter v korelaciji z bazo CVE in novimi znanimi ranljivostmi, ki se pojavijo v zaznani PO, opozarja odgovorne v oddelku IT o potrebnih akcijah. Skrbi tudi za poročanje o IKT sredstvih podjetja. Prednosti omenjene storitve sta centralizacija popisa sredstev (programska in strojna oprema) ter neobremenjevanje virov posameznih sistemov, njena slabost pa je manjša natančnost zaznane PO za korelacijo s CVE.
3) Informativna spletna storitev, ki na podlagi namena uporabe, izbranega operacijskega sistema ter nameščene programske opreme predhodno oceni ranljivost sistema glede na znane CVE ranljivosti. Takšna storitev bi bila za podjetja uporabna predvsem pri odločanju, katero strežniško PO ter sistem izbrati za svojo standardno platformo glede na poslovne potrebe. Prednost tovrstne rešitve bi bila, da bi lahko preko uporabniškega vmesnika izbrali določeno PO in na osnovi tega dobili poročilo in trende popolnoma neodvisno od sredstev v organizaciji.

Predvsem prvi dve rešitvi omogočata veliko stopnjo avtomatizacije, kar je tudi eden od razlogov, da v svetu že obstaja nekaj komercialnih ponudnikov tovrstne opreme.

5.8.4 OVAL in pregledovalniki ranljivosti sistemov

V prejšnjih poglavjih sem zapisal vizijo, kako bi lahko naredili sisteme IKT varnejše s tem, da izberemo varnejšo programsko opremo. Trenutno že obstajajo tovrstne (komercialne) rešitve. Organizacija MITRE ima objavljen tudi spisek tistih, ki so skladni s standardom CVE [67].

Na tem mestu je potrebno omeniti tudi OVAL (Open Vulnerability and Assessment Language) [79]. OVAL je odprt, mednarodno podprt jezik za prenos informacij o informacijski varnosti. Razvit je bil za prenos javno dostopnih varnostnih vsebin, ki standardizira prenos informacij v celem spektru orodij in storitev. OVAL vključuje jezik za zapis podrobnih informacij o sistemih in celotno zbirko podatkovnih baz z informacijami o varnosti, ki jih vzdržuje skupnost.
Jezik standardizira tri glavne korake procesa ocenjevanja:

a) zapis konfiguracijskih informacij o sistemih za testiranje (nastavitve, programska oprema);
b) analizo stanja sistema (ranljivost, konfiguracija, stanje popravkov – patches, stanje sistema in podobno);
c) poročilo z rezultati ocenjevanja sistema.

S pomočjo OVAL-a lahko sistem za iskanje ranljivosti (scanner) pregleda računalniški sistem in poda poročilo o najdenih ranljivostih (korelacija s CVE in ostalimi registri znanih ranljivosti). S tem olajša delo vzdrževalcem sistemov in pomaga zmanjšati število znanih ranljivosti v sistemih.

6 Prenosne naprave v organizaciji

6.1 Uvod

Uvajanje prenosnih naprav pomeni nove priložnosti za organizacije. Zaposleni so bolj zadovoljni in produktivni, če imajo dostop do službene elektronske pošte, aplikacij in podatkov na njihovih pametnih telefonih in tablicah. Z dobro načrtovanim uvajanjem prenosnih naprav lahko podjetje dosega konkurenčno prednost pred tekmeci. V nadaljevanju bom predstavil nekaj statističnih podatkov s tega področja za slovenska podjetja ter navedel smernice za varno uvajanje prenosnih naprav v organizacije.

6.2 Dodelitev prenosnih naprav z mobilnim dostopom do interneta

6.2.1 Pregled statističnih podatkov po velikosti podjetij

Več kot polovica (61%) podjetij v Sloveniji je v letu 2012 svojim zaposlenim dodelila prenosni računalnik, tablični računalnik ali pametni telefon, ki je imel hkrati tudi dostop do interneta (prek USB-modema, podatkovne kartice s tehnologijo vsaj 3G). Med velikimi podjetji je bilo takih podjetij kar 94%, med srednje velikimi 80% in med malimi 56% podjetij (tabela 39).

Kljub visokemu deležu podjetij, ki so svojim zaposlenim dodelila prenosne naprave, je delež zaposlenih oseb, ki sta jim bila dodeljena prenosni računalnik ali pametni telefon (s tehnologijo vsaj 3G za dostop do interneta), znašal le 6% (vir: SURS).

Tabela 40 prikazuje dodelitev prenosnih naprav z mobilnim dostopom v finančnem sektorju. Statistični podatki kažejo, da je tu v povprečju 86% podjetij dodelilo svojim zaposlenim prenosno napravo z vsaj 3G tehnologijo za dostop do interneta. Med temi so mala podjetja iz finančnega sektorja dodelila omenjeno prenosno napravo v 62%, velika in srednja pa kar v 100%. Zanimivo je, da so v povprečju podjetja v finančnem sektorju dodelila prenosne računalnike in druge prenosne naprave z vsaj 3G tehnologijo kar dvakrat pogosteje (70%) kot ostala podjetja (34%).

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
D1: Dodelitev prenosnih naprav z vsaj 3G tehnologijo za dostop do interneta	61%	56%	80%	94%
D2:..Dodelitev prenosnih računalnikov z vsaj 3G tehnologijo	43%	38%	61%	87%
D3:..Dodelitev drugih prenosnih naprav z vsaj 3G tehnologijo	52%	46%	70%	90%
D4:..Dodelitev zgolj prenosnih računalnikov z vsaj 3G tehnologijo	10%	10%	10%	4%
D5:..Dodelitev zgolj drugih prenosnih naprav z vsaj 3G tehnologijo	18%	18%	19%	7%

D6:..Dodelitev prenosnih računalnikov in drugih prenosnih naprav z vsaj 3G tehnologijo	34%	28%	51%	83%
D7: Možnost dostopanja do javno dostopnih informacij na internetu	56%	50%	76%	91%
D8: Možnost dostopanja do sistema elektronske pošte podjetja	53%	47%	76%	93%
D9: Možnost dostopanja in spreminjanja dokumentov podjetja	28%	24%	42%	63%
D10: Možnost uporabe namenskih poslovnih aplikacij (npr. upravljanje naročil in nakupov, aplikacij, povezanih z ERP)	16%	12%	30%	56%

Tabela 39: Dodelitev prenosnih naprav z mobilnim dostopom do interneta, leto 2012 (vir: SURS)

	10 ali več zaposlenih	10–49 zaposlenih	50–249 zaposlenih	250 ali več zaposlenih
D1: Dodelitev prenosnih naprav z vsaj 3G tehnologijo za dostop do interneta	86%	62%	100%	100%
D2:..Dodelitev prenosnih računalnikov z vsaj 3G tehnologijo	79%	z	z	100%
D3:..Dodelitev drugih prenosnih naprav z vsaj 3G tehnologijo	77%	z	100%	z
D4:..Dodelitev zgolj prenosnih računalnikov z vsaj 3G tehnologijo	9%	z	-	z
D5:..Dodelitev zgolj drugih prenosnih naprav z vsaj 3G tehnologijo	7%	z	z	-
D6:..Dodelitev prenosnih računalnikov in drugih prenosnih naprav z vsaj 3G tehnologijo	70%	38%	83%	94%
D7: Možnost dostopanja do javno dostopnih informacij na internetu	z	z	100%	100%
D8: Možnost dostopanja do sistema elektronske pošte podjetja	81%	z	100%	z
D9: Možnost dostopanja in spreminjanja dokumentov podjetja	51%	29%	50%	78%
D10: Možnost uporabe namenskih poslovnih aplikacij (npr. upravljanje naročil in nakupov, aplikacij, povezanih z ERP)	26%	z	z	39%

Tabela 40: Dodelitev prenosnih naprav z mobilnim dostopom do interneta, finančni sektor, leto 2012 (vir: SURS)

6.3 Zakaj uporaba mobilnih naprav povečuje tveganja

Danes je popolnoma normalno, da zaposleni med delovnim časom v podjetje prinesejo svoje mobilne naprave (telefone, tablice) oziroma svoje zasebne naprave uporabljajo tudi za službene namene. Največkrat je to pregledovanje službene e-pošte, dostop do dokumentov in prezentacij, uporaba službene centrale SIP za cenejše klice v/iz tujine (telefonija IP) preko mobilnega telefona, dostop do ostalih sistemov v podjetju kot so: CRM, ERP, baza znanja ipd.

Poleg večje fleksibilnosti, odzivnosti in udobja pri delu to s seboj prinese večja tveganja za izgubo ali krajo občutljivih informacij (dokumenti podjetja, informacije o strankah, e-poštni naslovi, gesla, ...).

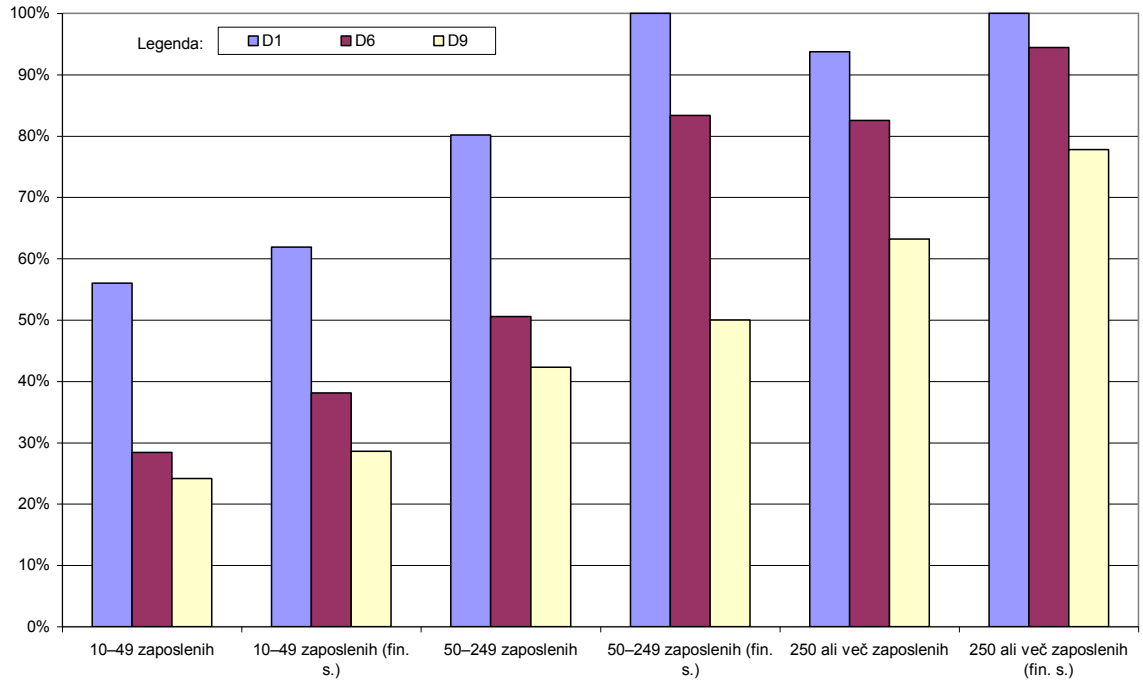


Tabela 41: Graf - dodelitev prenosnih naprav z mobilnim dostopom do interneta, primerjava podjetij v finančnem sektorju z ostalimi podjetji, glede na število zaposlenih, leto 2012 (vir: SURS)

6.4 Katera tveganja prinaša uporaba mobilnih naprav v organizaciji

Uporaba mobilnih naprav, predvsem tistih v osebni lasti zaposlenih (in obiskovalcev) za organizacijo prinaša naslednja tveganja [56].

1) Včasih so nad (zavarovanimi in upravljanimi) namiznimi računalniki in prenosniki administratorji IT tudi izven pisarne lahko imeli dober pregled in kontrolo. Danes pa z osebnimi mobilnimi napravami zaposleni lahko dostopajo do podatkov podjetja iz kateregakoli nezavarovanega omrežja, kar precej otežuje proces nadzora in uveljavljanje varnostnih ukrepov.

   Nat Kausik, direktor podjetja Bitglass, je izjavil: »Ko so organizacije imele navadne namizne računalnike, so jih upravljale. Nanje so naložile programsko opremo, jih zaklenile, tako da uporabnik na noben način ni imel možnosti spreminjati naložene programske opreme. Z mobilnimi napravami je ta pristop v osnovi postal nezadosten.«

2) Podatki iz mobilnih naprav so pogosto dostopni ali hranjeni tudi v oblaku. To dodatno otežuje skladnost mobilnih naprav, kajti organizacija je še vedno odgovorna za podatke, ki jih ponudnik storitev v oblaku omogoča, hrani ali upravlja za podjetja IT.

3) Uporaba mobilnih naprav prinaša bolj kompleksne tehnične in pravne vidike odgovornosti za podatke podjetja in osebne podatke zaposlenih ter strank.

4) »Nekatere spletne trgovine (podjetja, ki poslujejo preko spleta) sploh ne vedo, katere naprave imajo v omrežju in ali so te naprave osebna last ali last podjetja. Zato takšna podjetja tudi ne vedo, katere aplikacije so v podjetju v uporabi in do katerih informacij v zvezi s podjetjem te aplikacije lahko dostopajo. Ta težava se pojavi predvsem v podjetjih, ki nimajo standardov oziroma pravil, ki bi določala, katere naprave so lahko v uporabi, hkrati pa nimajo določenih jasnih pravil, na kakšen način lahko zaposleni uporabljajo naprave, katerih uporaba je v podjetju sicer dovoljena« meni Kevin Beaver, neodvisni svetovalec za varnost pri podjetju Principle Logic.

5) Ker oddelek IT ne upravlja z napravami, ki so last zaposlenih, podatki na teh napravah niso šifrirani, kar pomeni, da ima zlonamernež, če uporabnik napravo izgubi ali je naprava ukradena, zelo lahek dostop do podatkov, gesel in aplikacij organizacije. Prav tako ni možno na daljavo zbrisati podatkov organizacije, če takšna mobilna naprava pride v napačne roke.

6) Velika težava so lahko tudi zlonamerne aplikacije (virusi, trojanski konji, vohunsko programje ipd.), ki jih ima morda uporabnik nevede na svoji prenosni napravi. Ko se takšna naprava prijavi v omrežje podjetja, prej omenjene zlonamerne aplikacije lahko zbirajo promet v omrežju in ga pošiljajo na strežnike, ki jih upravlja zlonamernež.

7) Vodstvo organizacije se ne zaveda ali pa noče nameniti potrebnih sredstev za zagotavljanje skladnosti prenosnih naprav v organizaciji. Napačno dojemanje, da je zagotavljanje skladnosti prenosnih naprav in težav, ki pri tem nastanejo, zgolj v domeni oddelka IT, pogostokrat vodi v težavo, da oddelek IT ne more dosledno zavarovati podatkov organizacije, saj nima podpore vodstva.

Danes obstaja precej rešitev za celovito upravljanje prenosnih naprav (angl. mobile device management). Navadno je to kombinacija programske opreme in procesov, ki jih izvaja oddelek IT, poleg tega pa je potrebno na prenosno (mobilno) napravo namestiti posebno programsko opremo, ki služi celovitemu nadzoru in omogoča celovito upravljanje takšnih naprav s strani oddelka IT. Podrobneje o tem v poglavju 6.6.

V naslednjih dveh primerih je opisano, kako enostavno lahko napadalec izkoristi ranljivost pri uporabi neupravljane (mobilne) naprave.

Primer 1: Nepooblaščen dostop in izvajanje telefonskih klicev

Podjetje XX ima svojo centralo SIP za telefonijo IP. Ta za komunikacijo z mednarodnimi strankami in partnerji omogoča poceni klice v tujino in iz tujine.

Zaposleni v tem podjetju je na svoj lasten mobilni telefon naložil aplikacijo (klient SIP) in od oddelka IT izvedel, kako jo mora nastaviti, ter dobil geslo za njegov SIP dostop.

Ko je odšel na poslovno pot, je opravil še nekaj SIP klicev strank, pri čemer se je na internetno omrežje povezal preko nezavarovane brezžične točke (WiFi) na letališču. Naslednji dan je podjetje preko e-pošte iz centrale SIP prejelo opozorilo, da so prekoračili določeni znesek porabe.

Analiza dogodkov in dnevniških zapisov centrale SIP je pokazala, da je napadalec na letališču prestregel SIP geslo in uporabniško ime zaposlenega ter ga potem uporabil v svoje namene, pri čemer je opravil več kot 60 klicev. Podjetje je bilo oškodovano za okrog 190 evrov in ceno delovnega časa zaposlenih, ki so bili vključeni v ugotavljanje in odpravo incidenta. Z menjavo SIP gesla je bila ta težava odpravljena, vendar to še zdaleč ni bila zadostna rešitev problema. Kmalu so pripravili in sprejeli varnostno politiko za upravljanje mobilnih naprav.

Primer 2: izkoriščene ranljivosti zaradi neupravljanja prenosnega računalnika

Zaposlena v podjetju XY se je odpravila proti domu. Vmes se je ustavila na kavi s prijateljico. Medtem je prejela klic hčerke, ki je prejšnji večer pisala seminarsko nalogo na njenem službenem računalniku. Prosila je, naj ji preko storitve Dropbox[20] posreduje seminarsko nalogo, da jo še enkrat pregleda in natisne za šolske namene. Kot dobra mama je takoj vklopila prenosni računalnik, se povezala na nezaščiteno WiFi omrežje, pri čemer se ni zmenila za opozorilo ob prijavi v račun Dropbox, v katerem je pisalo, da je z varnostnim SSL[21] certifikatom nekaj narobe. Kljub opozorilu se je prijavila v svoj račun Dropbox ter hčerki posredovala njeno seminarsko nalogo. Medtem je zlonamernež prestregel njeno uporabniško ime in geslo za račun Dropbox in s tem tudi dostop do vseh dokumentov, ki jih je zaposlena hranila v računu Dropbox. V tem uporabniškem računu pa je zaposlena poleg zasebnih dokumentov hranila tudi pomembne tehnične in razvojne dokumente podjetja.

Škoda podjetja pri tem ni bila ocenjena, saj podjetje sploh ni vedelo, da je prišlo do vdora. Eventuelna škoda bo odvisno od tega, kateri dokumenti so v uporabniškem računu in če jih bo napadalec zlorabil oziroma zbrisal ter ali so bila v katerem od dokumentov zapisana tudi druga gesla in dostopi. Takšno nevarno stanje za škodne posledice lahko traja mesece ali celo leta, pri čemer nihče v podjetju sploh ne bo vedel, da jim odtekajo informacije in kje.

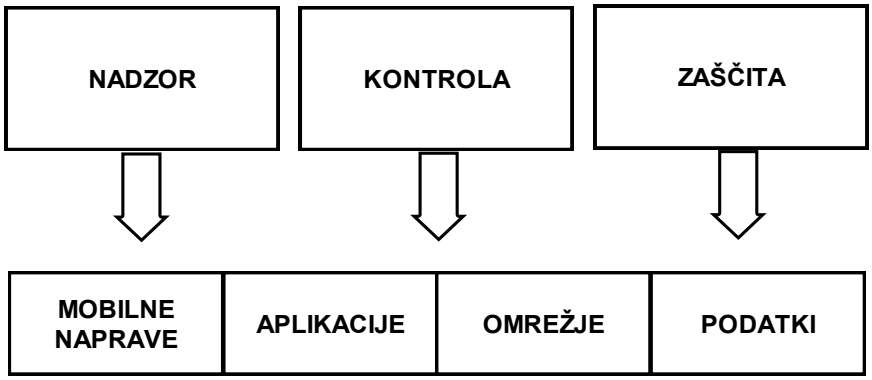
Ker prenosnik ni bil pravilno upravljan, oddelek IT v podjetju ne ve, da zaposlena uporablja svoj račun Dropbox, ki ni upravljan s strani podjetja. Ona si sicer na ta način olajša svoje delo, ne zaveda pa se nevarnosti, ki pri tem prežijo na varnost zaupnih informacij podjetja, v katerem je zaposlena. Gre za tako imenovani IT v

[20] Dropbox – storitev hranjenja in izmenjave datotek v oblaku (https://www.dropbox.com/) [70].
[21] SSL – Secure Socket Layer – povezava preko varnega protokola.

senci (angl. shadow IT), ko si zaposleni pomagajo pri svojem delu z dostopnimi storitvami in programi, oddelek IT podjetja pa tega ne upravlja.

6.5 Dobre prakse uporabe mobilnih naprav v poslovnem okolju

Celovito upravljanje prenosnih naprav zahteva nadzor naprav in kontrolo nad aplikacijami ter omrežjem z namenom zaščite podatkov organizacije (slika 22).



Slika 22: Ogrodje za mobilno upravljanje (povzeto po [92])

Organizacije naj bi upoštevale vsaj naslednja načela pri uporabi mobilnih naprav (povzeto po [51]):

1. Mobilna naprava naj ima nameščen protivirusni in protivohunski program.

2. Uporaba varnih komunikacijskih kanalov pomeni, da se za dostop do sistemov v podjetju uporablja VPN (virtualno privatno omrežje), saj je na nezaščitenih WiFi točkah mogoče enostavno prestrezati promet. Poleg močne enkripcije prometa lahko na strežniku VPN izvajamo analizo prometa in omogočimo/onemogočimo dostop do ostalih sistemov v podjetju glede na pravice uporabnika. Enostaven, a učinkovit koncept rešitve opisuje Copeland [2].

3. Uporaba močnih gesel in preverjanje dostopa pomeni, da je mobilna naprava varno zaklenjena in jo je mogoče uporabljati le, če poznamo geslo za odklepanje oziroma prijavo na napravo. Podatki na njej naj bodo šifrirani, obenem pa naj bo omogočeno oddaljeno brisanje podatkov v primeru , da je naprava ukradena ali izgubljena ali če zaposleni zapusti podjetje. Obenem je potrebno upoštevati, da se vsebina lahko samodejno zbriše z naprave, če uporabnik napravo prevečkrat poskuša odkleniti z napačnim geslom.

4. Nadzor nad aplikacijami pomeni, da na napravi ne teče nobena aplikacija, ki ni potrjena s strani oddelka IT v podjetju. Tako se prepreči morebitno uhajanje dokumentov iz podjetja – s strani zlonamerne aplikacije ali pa z načrtovanim dejanjem uporabnika mobilne naprave. Če je potrebno, naj se do sistema v podjetju raje omogoči priklop preko VPN in oddaljenega namizja. Tako so podatki vedno varno v podjetju, hkrati pa za branje

oziroma urejanje dostopni zaposlenemu preko mobilne naprave. Podjetja lahko sprejmejo tudi varnostne politike, ki prepovedujejo in/ali preprečujejo nalaganje datotek podjetja na mobilno napravo.

5. Brezžične dostopne točke organizacije naj bodo varovane in nastavljene tako, da usmerjajo promet ločeno od ostalega prometa v omrežju. Pri tem naj se uporabi požarni zid za blokiranje neželenega prometa ter kontrola vsebine prenosa. S tem se izognemo odtekanju informacij iz podjetja. Upravljanje obsega določanje ločenih pravic dostopa ali blokade (predvsem za povezane LAN in WiFi) za naprave, ki gostujejo ali niso poznane.

6. Izberite oziroma določite, katere mobilne naprave lahko zaposleni uporabljajo in jim jih pomagajte zavarovati. Naprave naj se ne povezujejo preko nevarovanih (odprtih) WiFi omrežij, brezžični vmesnik Bluetooth naj bo privzeto skrit oziroma ugasnjen, če ni v uporabi z brezžičnimi slušalkami. Skratka, mobilne naprave naj imajo privzeto izklopljene vse (predvsem brezžične) vmesnike, ki niso potrebni v danih okoliščinah.

7. Izvajajte redne letne penetracijske teste na mobilnih napravah. V ta namen najemite zunanje strokovnjake, ki vam bodo pomagali odkriti ranljivosti in jih tudi odpraviti.

Vse to je možno centralno varovati in upravljati s primernim celovitim upravljanjem mobilnih naprav v organizaciji.

6.6 Obvladovanje mobilnih naprav v organizaciji

6.6.1 Uvod

Upravljanje mobilnih naprav (angl. mobile device management – MDM) s strani organizacije omogoči posebna programska oprema za upravljanje mobilne naprave (MDM), ki jo oddelek IT namesti na mobilno napravo. S pomočjo te programske opreme lahko oddelek IT centralno upravlja in nadzira stanje mobilne naprave.

Ta programska oprema potem poskrbi, da se uporabijo varni vsebniki in profili na napravi. Ključno je, da se varno ločijo zasebni in poslovni podatki ter aplikacije. To pomeni, da se podatki, elektronska pošta in aplikacije, ki so lahko v uporabi v podjetju šifrirajo, in ločijo od podatkov uporabnika in njegovih aplikacij. Za to je potrebno namestiti dodatno programsko opremo na mobilno napravo s strani oddelka IT v organizaciji. Uporabnik pa nato le izbere profil uporabe naprave (zasebni ali službeni).

Tako so potem službeni podatki in dostopi varno shranjeni na mobilni napravi, hkrati pa jih oddelek IT lahko briše in nadzira na daljavo. Obenem je zagotovljena zasebnost uporabnika, saj do njegovih kontaktov, slik, dokumentov in aplikacij oddelek IT ne more dostopati. S tem je vzpostavljen tudi pravni vidik zagotavljanja zasebnosti zaposlenih v organizaciji.

V osnovi gredo rešitve na področju upravljanja mobilnih naprav v dve smeri. Ena so ločeni uporabniški profili (zasebni, delo ipd.), druga pa je virtualna namizna infrastruktura, ki je v bistvu razširitev že znanih virtualnih namizij za uporabo na mobilnih napravah.

6.6.2 Varni ločeni aplikacijski vsebniki (angl. application containers)

Kot je napisano že v uvodu tega podpoglavja, se na napravi ustvarijo ločene identitete (angl. identities, profiles), ki so med sabo nevidne in šifrirane vsaka s svojim ključem. Vsaka identiteta ima možnost dostopa le do svojih podatkov v vsebniku in do aplikacij, ki so na voljo v tej identiteti.

Če pride v nekem profilu do okužbe z virusom, je ogrožen le ta profil, zato z namenom odstranitve virusa enostavno zbrišemo celoten okuženi profil.

Danes na tem področju že obstaja nekaj rešitev, vendar pa je možnosti za nadaljnji razvoj še veliko.

Najvidnejša predstavnika teh rešitev sta Samsung KNOX [83] in Android for Work [59], ki sta običajno za manjše organizacije brezplačna. Obstaja pa tudi nekaj drugih plačljivih rešitev, med katerimi je med boljšimi Sophos Mobile Control [87], ki med drugim zna upravljati tudi Samsung KNOX.

Rešitvi omogočata:

- ločevanje poslovnih in zasebnih podatkov uporabnika;
- omogočata razširitve in prilagoditve s strani oddelka IT v podjetju;
- upravljanje mobilne naprave in podatkov v oblaku;
- večnivojsko zaščito naprave (zaščita zagona naprave, zaščita jedra operacijskega sistema, varnostne razširitve, dvostopenjsko avtentikacijo vključno z branjem prstnih odtisov).

6.6.3 Navidezna namizna infrastruktura

Vse organizacije ne želijo nameščati programske opreme na mobilne naprave svojih zaposlenih iz naslednjih razlogov:

- Ne želijo imeti dodatnih stroškov s programsko opremo in podporo.
- Uporabnike oziroma lastnike mobilnih naprav skrbi poseg v njihovo zasebnost.
- V podjetju že imajo vpeljane procese, s pomočjo katerih zaposleni lahko dostopajo do svojih namizij preko tankih odjemalcev in varne povezave.

V tem primeru se uporabi navidezna namizna infrastruktura (angl. virtual desktop infrastructure - VDI). Ta omogoča, da preko posebnega odjemalca (aplikacija, ki se namesti na mobilno napravo) in varne (VPN) povezave ter seveda z avtentikacijo uporabnik lahko odstopa do svojega namizja, ki navadno teče v varnem podatkovnem centru podjetja.

Tako se poslovne aplikacije in podatki varno nahajajo v podatkovnem centru, uporabnik pa ima dostop do njih preko oddaljenega namizja. Na ta način se podatki nikoli ne hranijo na napravi.

Slabosti tega načina so lahko:
1. počasno delovanje, če uporabnik nima dovolj hitre podatkovne povezave;
2. slaba uporabniška izkušnja, če aplikacije ne zaznajo, da je namizje prikazano preko mobilne naprave (multi-dotik, premajhni gumbi in ikone).

Seveda pa bo s prilagojenimi mobilnimi klienti in strežniško aplikacijo za serviranje navideznega namizja uporaba le-tega preko mobilnih naprav vse bolj prijazna.

6.7 Ključni koraki pri uvedbi upravljanja mobilnih naprav

Če organizacija načrtuje upravljanje mobilnih naprav, mora imeti najmanj:
1) strategijo upravljanja mobilnih naprav;
2) tudi za mobilne naprave dovolj podroben popis teh naprav (tako kot za ostale naprave);
3) razdelan življenjski cikel upravljanja (identifikacija naprave, prijava naprave v upravljanje, upravljanje, umik iz procesa upravljanja);
4) določeno strategijo za upravljanje programske opreme na napravi;
5) določeno varnostno politiko upravljanja naprav;
6) vpeljan proces zaščite podatkov na napravi;
7) zagotovljen nadzor (monitoring) naprav in podporo uporabnikom upravljanih naprav;
8) določena finančna sredstva namenjena za izvajanje zgoraj navedenih procesov.

Tako kot za ostalo opremo je za prenosne naprave še toliko pomembneje, da jih organizacije uvajajo premišljeno in načrtno ter se zavedajo pozitivnih in negativnih posledic njihovega uvajanja.

To velja tudi za pravila uporabe zasebnih mobilnih naprav v službene namene. Poleg pozitivnih faktorjev, kot so večja fleksibilnost in razpoložljivost zaposlenih, je potrebno poudariti, da varovanje podatkov in morebitna pomoč uporabnikom s seboj prineseta tudi določene stroške, kljub temu da se na prvi pogled zdi, da organizacija nima dodatnih stroškov, če mobilne naprave kupijo zaposleni sami in so njihova lastnina.

Priporočljivo je, da organizacija vpeljuje uporabo (predvsem zasebnih) mobilnih naprav načrtno in v skladu s postavljenimi varnostnimi politikami. Temu naj nameni tudi primerna finančna sredstva.

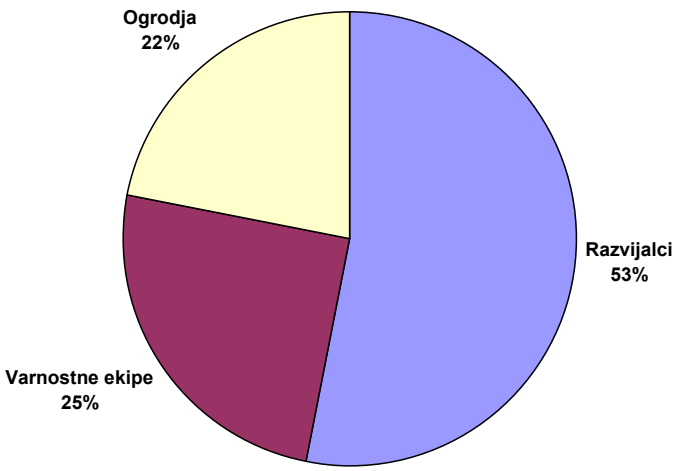
Te smernice lahko smiselno in brez dodatnih stroškov vpelje že majhna zagonska organizacija in jih glede na hitrost rasti dopolnjuje na način, da na koncu celovito upravlja mobilne naprave v skladu z napisanimi smernicami.

Pri velikih organizacijah pa je potrebno začeti od zgoraj navzdol. To pomeni s podporo in zavezo vodstva ter dodelitvijo potrebnih (tudi finančnih) sredstev za uvedbo in izvajanje učinkovitega upravljanja mobilnih naprav.

7 Razvoj in vzdrževanje programske opreme

7.1 Uvod

Raziskava med šeststo strokovnjaki na področju IT v letu 2015 je pokazala, da jih 53% meni, da so za varnost aplikacij v prvi vrsti odgovorni razvijalci, 25% strokovnjakov meni, da so za to primarno odgovorne ekipe za varnost ter 22%, da so za varnost aplikacij odgovorna razvijalska ogrodja [93].



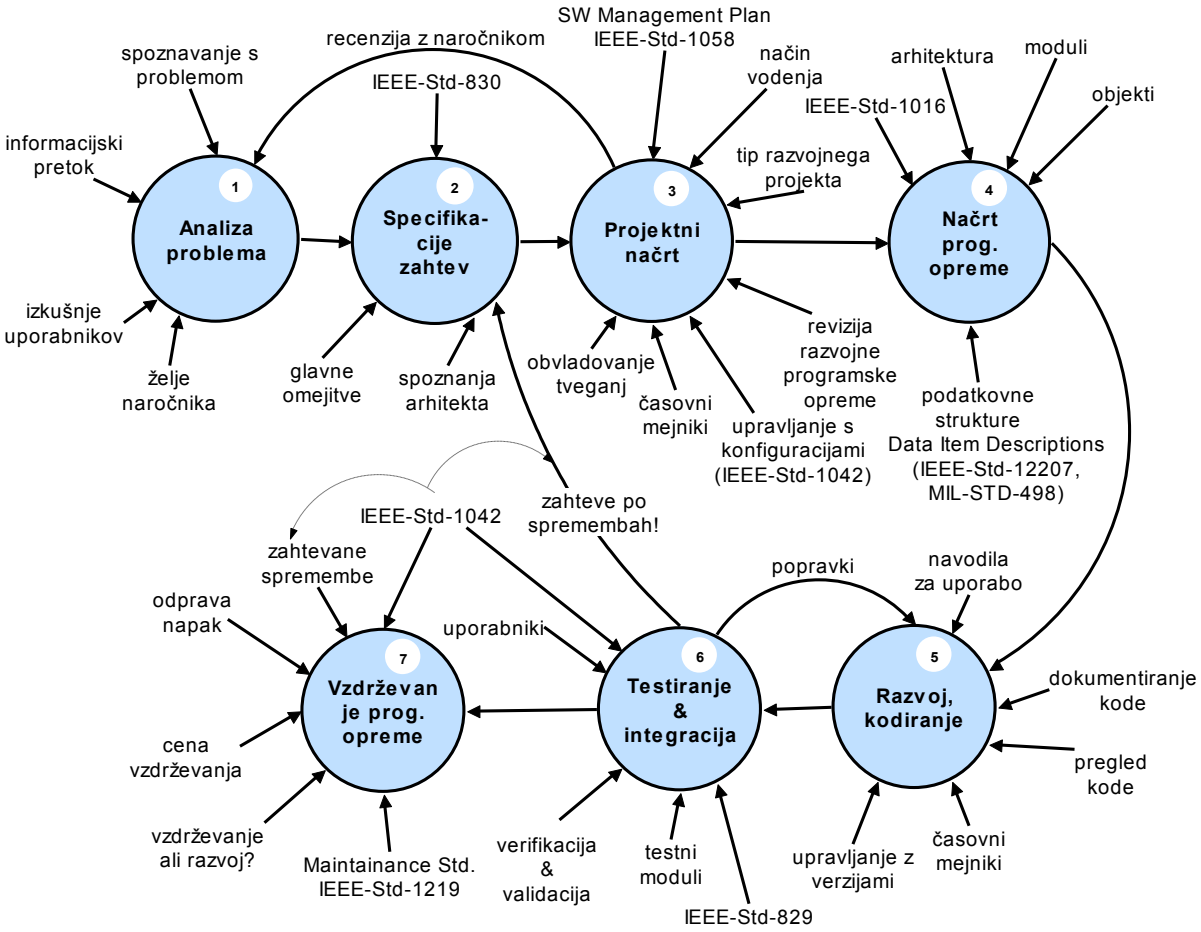
Slika 23: Raziskava: Kdo je odgovoren za varnost aplikacij? (vir: DZone [93])

Amy Zegart, poddirektorica centra za nacionalno varnost (CISAC) v ZDA, ocenjuje, da je v programski kodi danes na vsakih 2.500 vrstic kode vsaj ena napaka, ki lahko kritično vpliva na varnost aplikacije [98].

Tudi Howard [25] meni, da mora biti varnost načrtovana in implementirana v proizvode že na samem začetku razvojnega procesa. To povečuje pomembnost vzpostavitve celovite varnostne podpore razvojnemu procesu programske opreme z namenom zagotavljanja zaupnosti, celovitosti in razpoložljivosti obdelanih ter shranjenih podatkov ter s tem dodane vrednosti za naročnike oziroma uporabnike te programske opreme.

7.2 Ključni procesi in standardi

V tem, poglavju bom poskušal na kratko predstaviti, katere aktivnosti tvorijo projekt razvoja programske opreme. Shema na sliki 24 je nastala po izvlečkih iz knjig [48] in [43] Umestil sem tudi lastno razumevanje problematike ter izkušnje z razvojem in vodenjem projektov, ki imajo za cilj razvoj ali vzdrževanje programske opreme.



Slika 24: Shema cikla razvoja programske opreme (vir: lasten)

Z oznakami (številke 1 do 7) so navedeni ključni procesi v okviru izvedbe projekta razvoja programske opreme (v nadaljevanju RPO) od začetka do konca, puščice pa nakazujejo informacije, ki jih moramo upoštevati, ter ukrepe, ki jih izvajamo na posameznem koraku.

Shema kaže, kako nevarno je, če na začetku ne naredimo dobre analize, specifikacije zahtev [27] in projektnega načrta ali če ne naredimo podrobne recenzije z naročnikom pred izvedbo. Posledice so stroškovne narave, saj s tem po nepotrebnem povečujemo stroške projekta (prehod s točke 6 nazaj na točko 3). Naročnik lahko dobi programsko opremo, ki ne ustreza njegovim zahtevam in pričakovanjem (bolj ustreza zamislim izvajalca). V najslabšem primeru projekt propade še pred njegovim zaključkom.

Hvala je zapisal [26]:
Glede uspešnosti informacijskih projektov obstajajo različne ocene in le malo relevantnih raziskav, podprtih s podatki. Pogosta je ocena, da se informacijski projekti delijo v razmerju 25 : 25 : 50 – le četrtina jih v celoti doseže zastavljene cilje, četrtina jih uspe pogojno, kar pomeni, da so dosegli dovolj zadanih ciljev, polovica pa je popolnoma neuspelih in njihovi rezultati nikoli ne zaživijo.

Kot vidimo na sliki, sem dal velik poudarek standardom, saj je že Fairley [24] ugotovil, da so standardi ogrodja, ki omogočajo kreativnim ljudem rešiti težave. Brez ogrodja (standard), ki služi kot vodilo do uspeha, lahko postane kreativnost brezsmiseln kaos.

Vendar je treba opozoriti, da tudi standardi in metodologije niso čudežni ključ za uspešen RPO. Torej je potrebno tudi standarde upoštevati razumno, kot ugotavlja [26]: *"Še slabše, kot da projekt propade zaradi neuporabe metodoloških prijemov, je namreč to, da propade zaradi prevelike rigidnosti pri tem."*

Poleg splošnih IEEE standardov obstajajo tudi komercialni in vojaški standardi (MIL-STD-498, IEEE/EIA 12207.0, IEEE/EIA 12207.1, IEEE/EIA 12207.2), ki so prav tako dober vodič do uspešnega zaključka projekta [43, str. 35].

Da bi bili standardi učinkoviti, morajo vsi, od vključno najvišjih managerjev do zadnjih v verigi zaposlenih, razumeti [54]:

a) kako njihovo delo prispeva k ciljem organizacije (poslanstvo);
b) kako njihova programska oprema prispeva k poslanstvu;
c) kako standardi vplivajo na kakovost programske opreme in
d) kako standardi vplivajo na uspeh poslanstva.

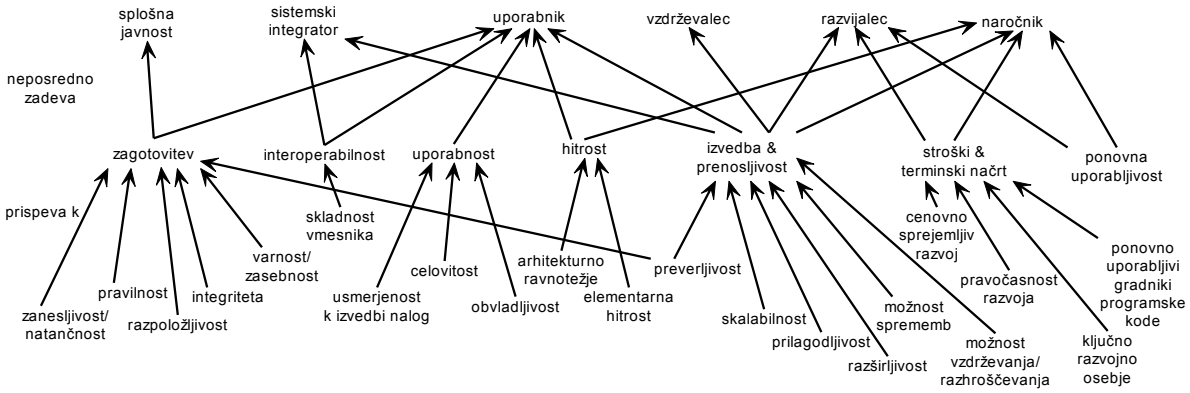
Zanimiv procesni pristop pri razvoju varne PO predlagajo Nunes, Belchior in Albuquerque, ki so omenjeni proces poimenovali proces za podporo varnosti programske opreme [11]. Proces temelji na uporabi modela SSE-CMM [34], standardov ISO/IEC 15408 [29, 30, 31], ISO/IEC 27002 [40] in metode OCTAVE (angl. the operationally critical threat, asset and vulnerability evaluation) [19]. Bistvena značilnost tega procesa je, da uporablja najboljše pristope omenjenih modelov in standardov, hkrati pa ostaja preprost in enostaven za praktično uporabo.

7.3 Kakovost programske opreme

Vsi sodelujoči v razvoju programske opreme imajo svoje zahteve (kupec nizko ceno, uporabnik varnost in hitrost, razvijalec lahko vzdrževanje, razvojno podjetje čim večji dobiček, zadovoljne stranke ipd.).

To lahko dosežemo predvsem s kakovostjo na nivoju celotne programske rešitve. Pri tem se moramo zavedati, da je ena od največjih nevarnosti programskega inženiringa preveliko poudarjanje le določenih atributov kakovosti (npr. hitrosti) na račun drugih, prav tako pomembnih lastnosti (npr. razširljivosti in prenosljivosti) [1].

Pomemben cilj dolgoročnega RPO bi morali biti primerno uravnoteženi atributi, ki jih vidimo na sliki 25.



Slika 25: Atributi kakovosti programske opreme po posameznih akterjih (povzeto po Boehmu [1])

7.4 Pogoste napake pri razvoju PO in kako jih preprečiti

Po nekaterih statističnih informacijah [98] naj bi bila v povprečju na vsakih 2500 vrstic programske kode napaka, ki naredi to PO ranljivo.

Razvijalci bi morali poznati najpogostejše napake, ki nastanejo v fazi razvoja, in biti sposobni takšne napake tudi predvideti in se jim izogniti.
V nadaljevanju je naštetih nekaj najbolj tipičnih napak, ki se zgodijo v prvih fazah razvoja in povzročijo najpogostejših 10 tipov ranljivosti programske opreme [80]:

1. Vrivanje programske kode (angl. code injection). Sem spada vrivanje SQL, OS in LDAP programske kode. To se zgodi zaradi slabega preverjanja vhodnih podatkov. V podatke lahko zlonamerneže doda ukaze, ki tam niso bili predvideni, in s tem prelisiči "prevajalca ukazov", da naredi nekaj, česar ne bi smel.

2. Šibka avtentikacija in upravljanje sej (angl. weak authentication and session management). Avtentikacijske funkcije in upravljanje sej pogosto niso pravilno vgrajeni. To pa napadalcu omogoči zlorabo gesel, ključev, sejnih žetonov ali celo izrabo pomanjkljivosti aplikacije na način, da se (napadalec) predstavlja kot nek drug uporabnik.

3. Večdomensko izvajanje kode (angl. cross site scripting, XSS) se lahko zgodi, če aplikacija ne preverja vira podatkov in potem te podatke brez ustreznega preverjanja pošlje brskalniku. To omogoča izvajanje kode v žrtvinem brskalniku, s čimer napadalec lahko prevzame sejo uporabnika, povzroči razobličenje spletne strani ali pa preusmeri uporabnika (žrtev) na škodljivo spletno stran.

4. Nezavarovane direktne reference na objekte (angl. insecure direct object references) so lahko zlorabljene takrat, ko razvijalec izpostavi interni vir, kot je na primer datoteka, mapa ali ključ podatkovne baze. Brez pristopne kontrole ali

druge zaščite lahko napadalec manipulira s temi referencami in nepooblaščeno dostopa do podatkov.

5. Pomanjkljive varnostne nastavitve (angl. security misconfiguration) aplikacije, ogrodij, aplikacijskega strežnika, spletnega strežnika, podatkovnega strežnika, platforme. Potrebno je paziti, da so implementirane in vzdrževane varne nastavitve, kajti privzete nastavitve pogosto ne zagotavljajo zadostne mere varnosti. Prav tako je potrebno poskrbeti, da je omenjena programska oprema posodobljena.

6. Izpostavitev občutljivih podatkov (angl. sensitive data exposure). Mnoge spletne aplikacije občutljivih podatkov, kot so kreditne kartice, davčne številke in avtentikacijski podatki (npr. uporabniško ime in geslo), ne zavarujejo na primeren način. Posledično lahko napadalec slabo zaščitene podatke ukrade ali spremeni, izvrši goljufijo s kreditno kartico, izvede krajo identitete ali drugo kaznivo dejanje. Občutljivi podatki morajo biti posebej zaščiteni z enkripcijo tako ob zapisu kot ob prenosu. Posebna previdnost velja pri izmenjavi teh podatkov s spletnim brskalnikom.

7. Manjkajoča pristopna kontrola do funkcij (angl. missing function level access Control). Večina spletnih aplikacij preverja pravice dostopa do funkcij, preden prikaže to funkcionalnost v uporabniškem vmesniku. Prav tako mora aplikacija na strežniku izvesti enako kontrolo pravic, ko pride do dostopa do teh funkcij. Če takšni zahtevki (angl. requests) niso preverjeni, lahko napadalec ponaredi zahtevke in dostopa do teh funkcij brez primerne avtorizacije.

8. Večdomensko ponarejanje zahtev (angl. cross site request forgery, CSRF). CSRF napad prisili brskalnik prijavljene žrtve, da pošlje ponarejen HTTP zahtevek, vključno s sejnim piškotkom in vsemi drugimi avtomatično vključenimi avtentikacijskimi informacijami, na strežnik ranljive aplikacije. To omogoča napadalcu prisiliti žrtvin brskalnik, da generira zahteve, za katere spletna aplikacija misli, da gre za legitimne zahteve s strani žrtve.

9. Uporaba gradnikov z znanimi ranljivostmi (angl. using components with known vulnerabilities). Gradniki, kot so knjižnice, ogrodja in drugi programski moduli, skoraj vedno tečejo s polnimi privilegiji aplikacije. Če pride do zlorabe ranljive komponente, lahko takšen napad povzroči resno izgubo podatkov ali prevzem strežnika s strani napadalca. Aplikacije, ki uporabljajo gradnike z znanimi ranljivostmi, lahko popolnoma spodkopljejo svoje obrambne mehanizme in omogočijo več različnih napadov na aplikacijo ali celo na strežnik.

10. Nepreverjene preusmeritve in posredovanje (angl. unvalidated redirects and forwards). Spletne aplikacije pogosto preusmerjajo in posredujejo uporabnike na druge spletne strani ali portale, pri čemer uporabljajo nepreverjene podatke za določitev ciljne strani. Brez ustreznega preverjanja lahko napadalci preusmerijo žrtve na "phishing" strani, spletne strani z zlonamerno programsko opremo ali pa uporabijo posredovanje za nepooblaščen dostop do strani.

7.5 Smernice za razvoj varnih aplikacij

Na osnovi raziskav in OWASP-ove lestvice najpogostejših desetih ranljivosti [80] lahko z naslednjimi smernicami razvojni inženirji že pri razvoju preprečijo več kot 80% potencialnih ranljivosti v PO, ki jo razvijajo. Povzeto po smernicah [93, str. 6-8]

7. Zavarujte SQL podatkovno bazo pred injiciranjem kode. Kljub temu da je to ena najpogostejših ranljivosti, jo je moč dokaj enostavno zaznati in odpraviti s parametriziranjem SQL stavkov ter s tem tolmaču ukazov dati jasna navodila, kateri del SQL stavka je ukaz in kateri del so podatki.

8. Kodiranje podatkov (LDAP, XML, Xpath, XSS). Vrivanje SQL je le en tip napada z vrivanjem kode. Ostale napade, kot so LDAP, XML, XPath vrivanje, OS vrivanje ukazov in še posebej JavaScript vrivanje (večdomensko izvajanje kode), je veliko težje odpraviti.

   Rešitev za odpravo teh ranljivosti je ločitev ukazov od podatkov. Tega ni mogoče doseči tako enostavno kot pri odpravi vrivanja SQL. Zato je potrebno zagotoviti, da so podatki preverjeni in "varni", preden jih posredujemo zunanjemu tolmaču ukazov, kot je XML razčlenjevalnik, ukazna vrstica operacijskega sistema (OS) ali brskalnik. To dosežemo s kodiranjem podatkov, preden jih posredujemo tolmaču ukazov na način, da tolmač ukazov v podatkih ne bo prepoznal izvršljivih ukazov. Za izvedbo omenjenega ukrepa je potrebno poznati kodiranje ubežnih pravil za vsak tolmač ukazov posebej in jih pravilno uporabiti v določenih kontekstih (HTML, JavaScript, XML, CSS). Paziti je potrebno tudi, da ne pride do dvojnega kodiranja.

9. Validacija podatkov pred uporabo oziroma shranjevanjem na strežniku. Vedno je potrebno preveriti veljavnost vhodnih podatkov na strežniku. Ni dovolj, da se zanašamo, da je to opravil že odjemalec oziroma klient. Kjer je možno, uporabimo regularne izraze za definiranje dovoljenih vhodnih vrednosti.

10. Pristopna kontrola naj bo privzeto nastavljena za zavrnitev (avtorizacija). To pomeni, da je dostop do vseh podatkov in funkcij v osnovi zavrnjen ter se vsakič znova preveri, ali ima uporabnik pravice za dostop (avtentikacija, avtorizacija). Sama implementacija naj bo na strežniku v centralni knjižnici za upravljanje in ne razsejana po celotni poslovni logiki. S tem je mnogo lažje revidirati in nadgrajevati pravila. Za odločanje uporabljamo le podatke na strani strežnika, ki so bili preverjeni in so tako varni za uporabo.

11. Vnaprejšnje vzpostavljanje identitete. Za upravljanje avtentikacije in seje je bolje kot svoje prilagojene rešitve uporabiti preverjeno ogrodje. Če uporabljeno aplikativno ogrodje za to ne poskrbi zadovoljivo, si lahko pomagamo s knjižnicami, kot je Apache Shiro [60]. Kjer je možno, vgradimo večnivojsko avtentikacijo. Če smo odvisni le od uporabniškega imena in gesla, poskrbimo za primerno dolžino in kompleksnost gesel. Prav tako je potrebno uporabniška imena (še zlasti, če so to elektronski poštni naslovi) in gesla primerno šifrirati pred shranjevanjem.

Pozornost velja tudi pri funkcijah za obnovo gesla v primeru, da ga uporabnik pozabi. Tu je pomembno vgraditi dobra varnostna vprašanja ter verifikacijo odgovorov uporabnika. Uporabniku nato žeton za ponastavitev gesla pošljemo po drugem kanalu (elektronska pošta, SMS ipd.).

12. Zaščita podatkov in zasebnosti. Poleg pristopne kontrole (točka 4) in revidiranja (točka 7) je za zaščito podatkov in zasebnosti pomembno šifriranje podatkov v prenosu, ob shranjevanju in med obdelavo. Za spletne in mobilne aplikacije to pomeni, da pri prenosu podatkov vedno uporabljamo SSL/TLS kanal.

    Pri šifriranju pa se je potrebno izogibati najpogostejšim napakam, in sicer:
    a) da v osnovi pozabimo šifrirati podatke;
    b) da poskušamo izumiti svoj algoritem šifriranja;
    c) da uporabljamo slabo upravljanje s ključi in drugimi koraki pri nastavitvah standardnih knjižnic.

    Zadnja težava je razkrivanje podatkov med obdelavo. V zvezi s tem je potrebno paziti, da ne shranjujemo nešifriranih podatkov v začasne datoteke ter ne vključujemo občutljivih informacij v dnevniške datoteke. Pazljivost je potrebna tudi pri shranjevanju v delovni spomin.

13. Dnevniški zapisi in zaznavanje vdorov. Vodenje dnevniških zapisov ni pomembno le za odpravljanje težav in razhroščevanje, temveč je odločilnega pomena tudi za revidiranje aktivnosti, detekcijo vdorov (varnostnemu inženirju pove, kdaj je bil sistem napaden) in forenziko (ugotavljanje, kaj se je dogajalo po vdoru v sistem). Vedno je priporočljivo zapisati naslednja dejstva: kdaj je prišlo do vdora (časovni žig), kdo ga je izvedel (uporabniško ime), kje (IP naslov uporabnika), kaj natančno se je zgodilo (podrobnosti dogodka).
    Paziti je potrebno, da ne beležimo podatkov, kot so številke kreditnih kartic, gesla, osebni podatki, avtentikacijski podatki ipd).

    Upoštevati je potrebno tudi možnost ponarejanja dnevniških zapisov, saj napadalci v primeru, ko vedo, da se bo dogodek beležil, vrinejo dodatne kontrolne znake ali JavaScript ukaze, s čimer poskušajo zakriti aktivnosti. Zato tudi za dnevniške zapise velja, da je potrebno podatke enkodirati, preden jih zapišemo v dnevnik (točka 3).

14. Uporabljajte preverjena in posodobljena ogrodja ter knjižnice za uvedbo varnosti. Kljub temu da imajo mnoge knjižnice in ogrodja znane ranljivosti, je dostikrat bolje poiskati najboljše med njimi in jih uporabiti pri vgrajevanju varnosti, kot pa izumljati "toplo vodo" oziroma iskati svoje rešitve.

    Pomembno je, da spremljamo morebitne znane ranljivosti, ki se pojavijo v teh ogrodjih, ter poskrbimo tudi za popravke in nadgradnje.

15. Pravilno upravljanje napak (angl. error handling) in izjem nam lahko pomaga odkriti varnostne ranljivosti in preprečevati izpade sistema. Potrebno je paziti, da ne pride do odtekanja informacij. Izpis sledov sklada (angl. stack trace)

napadalcu nudi mnogo preveč tehničnih informacij o sistemu in okolju, ki jih napadalec lahko izkoristi pri nadaljnjih poskusih napada. Prav tako je bolje namesto opozorila "napačno uporabniško ime" ali "napačno geslo" uporabiti opozorilo "napačno uporabniško ime ali geslo", saj bo takšno opozorilo uporabnikom v pomoč, napadalcu pa s tem damo manj informacij.

Manjkajoče ali nekonsistentno upravljanje z napakami lahko povzroči, da resne napake niso zaznane. Lahko vodi celo do nepredvidljivega delovanja ali izpada aplikacije. Raziskave kažejo, da lahko manjši napačni ukrepi pri upravljanju napak vodijo do katastrofalnih posledic v velikih sistemih [14].

16. Uvajanje testiranja varnosti že v sam razvojni postopek. Varnostni pregledi naj bodo vključeni že v preglede izvorne kode (angl. code reviews) ter naj bodo tudi avtomatizirani v postopku neprekinjene integracije (angl. continous integration) in neprekinjenega vključevanja (angl. continuous delivery).

    Poskrbeti je potrebno za dobre avtomatizirane teste enot in integracijske teste, ki pokrivajo varnostne funkcije in kontrole (avtentikacija, kontrola pristopa, revidiranje ipd.) ter kritične poslovne funkcije (koda, ki upravlja z denarjem, zasebni podatki, izmenjani tajni podatki in administrativne funkcije).

    Za izvedbo takšnih testov obstaja precej rešitev in ogrodij, seveda pa je potrebno te dodatne teste izvesti že v fazi načrtovanja projekta in jih vključiti v časovno in stroškovno tabelo. Zavedati se je treba, da je odpravljanje tovrstnih napak v produkcijskih sistemih tisočkrat dražje.

Varnost pri razvoju programske opreme je močno odvisna od vodstva organizacije oziroma naročnika projekta, saj bi ta praviloma moral že v fazi zasnove projekta postaviti smiselne zahteve za zagotavljanje varnosti. V takšnem primeru bo to vračunano v časovne in stroškovne postavke. Naročnik se mora zavedati, da bo to veliko bolj optimalno, kot če bi zahteve po varnosti izrazil kasneje, ko bo velik del razvoja že opravljen, ali še slabše, šele takrat, ko bi projekt že zaživel v produkcijskem okolju.

8 Priporočila za izboljšanje varnosti IKT v slovenskih organizacijah

8.1 Še nekaj uporabnih priporočil za organizacije

Poleg upoštevanja standardov, postavitve varnostnih politik in agilnega obvladovanja razvojnih projektov, so za učinkovitejše delovanje organizacij pomembne tudi spodaj predstavljene rešitve. Na tem mestu jih omenjam zaradi njihovih vplivov na varnost IKT v organizaciji. Lahke metodologije, družbena omrežja, IT v senci ter računalništvo v oblaku bom sicer opisal zgolj na kratko, saj njihova podrobnejša obravnava za predmetno delo ni ključnega pomena. Pomembno pa je, da ima odgovorno osebje organizacije tudi te rešitve "na seznamu" in jih prilagaja glede na velikost in potrebe organizacije.

Lahke metodologije

Predvsem za zagonska podjetja je pomembno, da se tako kot pri razvoju proizvodov in storitev ter vstopu na trg, tudi pri postavljanju varnostnih politik in procesov IKT čimbolj poslužujejo lahkih (angl. lean) metodologij [42]. Lahke metodologije pa niso namenjene le zagonskim podjetjem. Tudi velika podjetja lahko z njihovo pomočjo hitreje in učinkoviteje dosežejo željene rezultate. Bistvo metode je (povzeto po [42]):

1. Zapiši načrt A.
2. Prepoznaj najbolj tvegane točke načrta.
3. Načrt sistematično testiraj in izboljšuj.

Cilj je z minimalnimi potrebnimi sredstvi doseči učinkovito rešitev poslovnega problema. Ta lahko predstavlja uvedbo novega proizvoda na tržišče, uvedbo neprekinjenega objavljanja v razvojnem procesu IS, uvedbo sistema za obvladovanje informacijske varnosti ipd.

Družbena omrežja

Danes zelo razširjena družbena omrežja (Facebook, Twitter, Snapchat ipd.) se uporabljajo tudi v organizacijah. Nekatere organizacije namreč uporabljajo družbena omrežja za promocijo proizvodov in storitev ter za gradnjo prepoznavnosti.

Predlagam, da organizacija sprejme politiko, ki obravnava uporabo in omejevanje uporabe družbenih omrežij. Družbena omrežja namreč lahko vplivajo na varnost IKT organizacij. Razlogov je več:

1. Na tem področju se je v pretekosti že izkazalo, da je prihajalo do razširjanja neželjene in vohunske programske opreme preko družbenih omrežij.
2. Pregledovanje vsebin, slik in videoposnetkov uporablja vire organizacije (mrežna povezava, protivirusni in protismetni strežniški filtri ipd). Morda se na prvi pogled zdi to dejstvo malo pomembno, toda če si predstavljamo organizacijo z 250 ali več zaposlenimi, v kateri zaposleni v nekem kratkem časovnem obdobju odprejo veliko količino (npr. viralna sporočila) takšnih vsebin, lahko za nekaj časa zelo obremenijo ali celo ohromijo podatkovne povezave takšne organizacije ter s tem povzročijo počasno ali celo onemogočeno delovanje ostalih poslovnih sistemov in storitev.
3. Poveča se nevarnost družbenega inženiringa.

4. Lahko pride do nepotrebnega razkrivanja omrežne topologije in računalniških sistemov v organizaciji. S tem je morebitnemu zunanjemu napadalcu olajšano delo.
5. Zaposleni niso osredotočeni na svoje delo.

Priporočljivo je, da organizacija sprejme jasna pravila in politiko uporabe družbenih omrežij na takšen način, da ne omejuje uporabe tistim zaposlenim, ki uporabljajo družabna omrežja v poslovne namene organizacije, ostalim pa uporabo teh omrežij onemogoči.

IT v senci (angl. shadow IT)
V procesu rasti organizacije od zagonskega podjetja do velikega podjetja se pojavljajo različne potrebe po podpori procesov s strani IT. Mikro ali zagonsko podjetje je lahko zelo fleksibilno in mnogokrat uporabi brezplačne ali cenovno ugodne rešitve. Navadno zagonska in mala podjetja tudi nimajo oddelka IT. Ko pa podjetje zraste in poslovni procesi postanejo kompleksnejši nekatere rešitve, sicer za zagonsko podjetje povsem zadostne, zanj niso več primerne. To kar je bilo včasih za zagonsko organizacijo uporabna in morda tudi edina rešitev, ki si jo je organizacija lahko privoščila, je lahko v srednjem ali velikem podjetju del tako imenovanega IT v senci (angl. shadow IT).

Eno boljših definicij tega pojma sta leta 2014 zapisala Silic in Back [13]: *"IT v senci je trenutno narobe razumljen in relativno neraziskan pojav. Predstavlja vso strojno opremo, programsko opremo ali katerekoli druge rešitve, ki jih zaposleni uporabljajo znotraj organizacijske strukture, vendar za njihovo uporabo niso prejeli nobene uradne odobritve oddelka IT."*

Za zagonsko podjetje je nekaj običajnega, da sodelujoči v podjetju za izmenjavo in deljeno hranjenje datotek uporabljajo storitve, kot je npr. Dropbox [70]. Za srednje velika in velika podjetja pa so tovrstne rešitve lahko varnostni problem. Velika podjetja imajo navadno svoj oddelek, ki skrbi za rešitve IKT, med drugim tudi rešitve hranjenja in deljenja datotek. Če oddelek IT ne poskrbi za tovrstne rešitve, se lahko zgodi, da zaposleni v dobri veri učinkovitega opravljanja delovnih nalog, brez vednosti odgovornih in IT oddelka, uporabijo osebne račune že omenjene storitve Dropbox ali podobne storitve ter si na ta način olajšajo reševanje delovnih nalog. Ker podjetje nima nadzora nad osebnimi računi zaposlenih, lahko pride do odtekanja podatkov. Do takšnih posledic lahko pride tudi v primeru, ko zaposleni uporabijo svoje osebne elektronske račune za pošiljanje službenih sporočil. V določenem preteklem obdobju je bil to pogost pojav, kajti mnoge organizacije so imele omejitve glede velikosti poslanih ali prejetih priponk (angl. attachments), kar je povzročilo, da so zaposleni za izmenjavo takšnih sporočil (znotraj organizacije ali med organizacijami) bili večkrat primorani uporabiti osebne račune storitve Gmail. To je zopet povzročilo, da so podatki potovali po kanalih izven pristojnosti organizacije.

V to področje spada tudi uporaba osebnih telefonov in ostalih naprav v službene namene, nad katerimi oddelek IT organizacije nima nadzora.

Naštel sem nekaj primerov, ki jim lahko rečemo IT v senci. Menim, da večja kot je organizacija, večje varnostno tveganje predstavlja IT v senci, zlasti, če ga organizacija ne zaznava ter regulira s pomočjo varnostnih politik in drugih ukrepov.

Računalništvo v oblaku

Računalništvo v oblaku je hitro rastoča tehnološka paradigma, ki spreminja obstoječe računalniške koncepte. Računalništvo v oblaku ima številne prednosti, kot so ekonomski prihranki in prilagodljivost storitev, enostavno nastavljanje in prilagajanje potrebnih računskih virov ali virov shranjevanja podatkov ter obračunavanje po dejanski porabi, tako kot to je to značilno za sistem za oskrbo z električno energijo [5]. V praksi se je že večkrat izkazalo, da sta pri tovrstnih rešitvah varnost in zasebnost pogosto na udaru. Namreč enkrat ko podatki zapustijo omrežje organizacije, njen oddelek IT nima več neposrednega vpliva na varovanje teh podatkov, torej ne more več zagotavljati zaupnosti, celovitosti, razpoložljivosti, kot sem zapisal v poglavju 2.2. Predvsem je na udaru zaupnost, kajti zaradi kompleksnosti shranjevanja v oblaku običajne enkripcijske metode ni mogoče zagotoviti ustrezne stopnje zaupnosti [18].

Na podlagi rezultatov izvedenih raziskav so v tabeli 42 zbrane najpogostejše težave, ki pestijo ponudnike storitev v oblaku. Razdeljene so na pet področij, in sicer na varnostne standarde, omrežje, dostop do podatkov, tehnično infrastrukturo oblaka ter podatke.

Področje	**Težave**
Varnostni standardi	Pomanjkanje varnostnih standardov. Tveganja glede skladnosti. Pomanjkanje revizije. Pomanjkljive pravne podlage (dogovor o ravni storitve, odgovornost). Zaupanje med uporabniki oblačnih storitev in ostalimi deležniki v procesu prenosa podatkov v oblak.
Omrežje	Pravilna nastavitev požarnih zidov na omrežju. Pravilna nastavitev omrežja. Ranljivosti mrežnih protokolov. Odvisnost od internetne povezave (napadi).
Dostop	Prevzem oziroma kraja servisnih in uporabniških računov. Možnost zlorabe s strani notranjih oseb z dostopom do informacij. Avtentikacijski mehanizem. Privilegiran uporabniški dostop. Varnost brskalnikov.
Infrastruktura oblaka	Slaba varnostna implementacija vmesnika API. Kakovost storitve (samo hitrost, nizka cena)? Skupne ranljive točke sistemov. Zanesljivost ponudnikov (servisno osebje). Napačne varnostne nastavitve. Delitev virov med najemniki (možnost uhajanja informacij). Postavitev strežnikov in varnostne kopije (tudi fizična zaščita).

Podatki	Redundanca podatkov. Izguba in odtekanje podatkov. Lokacija podatkov. Obnova podatkov. Zasebnost podatkov. Zaščita podatkov. Dostopnost podatkov.

Tabela 42: Področja težav pri uporabi računalništva v oblaku (povzeto po [5])

Ne glede na to, da celotna problematika povezana z uporabo storitev v oblaku presega okvire tega dela, lahko organizacija na osnovi težav, zapisanih v tabeli 42, pred izbiro ponudnika storitev v oblaku pri potencialnem ponudniku preveri našteta področja ter se s tem poskuša izogniti težavam na teh področjih. Na ta način pri izboru verjetno ne bo odločala le cena storitve. Podrobnejše informacije in dodatna pojasnila organizacija najde v [5].

Pri računalništvu v oblaku velja omeniti tudi pravne vidike. Za nekatere dejavnosti je zakonsko predpisano, da morajo biti podatki hranjeni v državi, kjer podatki nastanejo, ali v zvezi držav, kot je Evropska unija. Zaradi porazdeljenega shranjevanja podatkov in geografsko razpršenih podatkovnih centrov ponudnikov storitev v oblaku, je lokacija hrambe v praksi pogosto vprašanje, ki ga je potrebno rešiti pred podpisom pogodbe.

8.2 Svetovni statistični podatki o posledicah incidentov

Po podatkih organizacij IT-Harvest in SafeNet Inc., ki zbirata javno dostopne informacije o vdorih in ukradenih ali izgubljenih zapisih,[22] naj bi bilo od leta 2013 do danes ukradenih ali izgubljenih več kot 4,75 milijarde zapisov. To pomeni več kot 3,5 milijona ukradenih oziroma izgubljenih zapisov vsako uro oziroma približno 42 ukradenih ali izgubljenih zapisov na sekundo. Zgovoren je tudi podatek, da je bilo med incidenti, ki so imeli za posledico razkritje podatkov, le štiri odstotke takšnih, pri katerih so bili zaseženi ustrezno šifrirani podatki, ki so bili tako za napadalca neuporabni [61].

Definicija pojmov:

Zapis je posamezen podatek, ki vsebuje občutljivo informacijo, kot je na primer naslov e-pošte, osebni podatek (ime, priimek, datum rojstva), podatek za avtentikacijo (uporabniško ime, geslo), davčna številka, številka kreditne kartice, ipd.

Izgubljen zapis je zapis, ki je bil razkrit kot posledica incidenta. Ta incident je lahko posledica izgubljene naprave s podatki (prenosni računalnik, nosilec DVD, USB ključ, telefon, ipd.).

Ukraden zapis je zapis, ki je bil razkrit kot posledica kakršnegakoli incidenta, ki ga je izvedel napadalec z motivom pridobitve zapisov. Navadno takšne podatke

[22] Zapisi lahko vsebujejo različne podatke, kot so naslovi e-pošte, osebne informacije, številke kreditnih kartic, finančne transakcije, uporabniška imena, gesla in podobno.

(zapise) uporabijo kriminalne združbe za svoje nadaljnje akcije (preprodaja podatkov, dostop do finančnih sredstev, novi vdori ipd.).

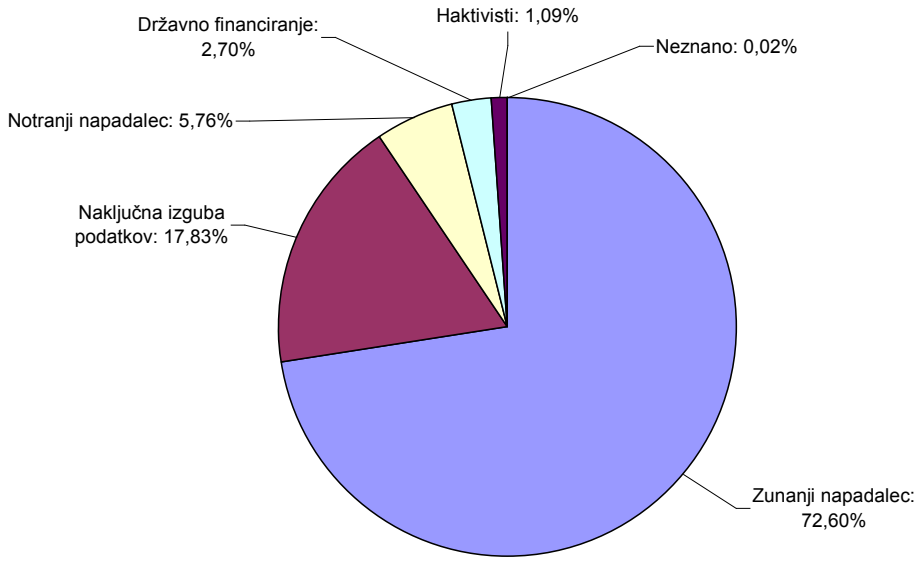
Dostopnih podatkov o posledicah incidentov [61] ni možno neposredno primerjati s podatki, objavljenimi na SURS [90], vendar vseeno lahko zaznamo določene podobnosti.

8.3 Pregled svetovnih statističnih podatkov glede na vir incidenta

Po podatkih BreachLevelIndex.com [61] je bilo v obdobju od leta 2013 do avgusta 2016 kar 72,60% incidentov s posledicami izgube ali kraje podatkov izvedenih s strani zunanjih napadalcev, v 17,83% je šlo za naključno izgubo podatkov, v 5,76% je bil vir incidenta notranji napadalec, v 0,02% pa je šlo za neznan vir napada (slika 26).

Zanimivo je, da je bilo 2,70% incidentov s posledicami izgube ali kraje podatkov izvedenih s finančno podporo posameznih držav. To je skoraj trikrat več, kot je bilo napadov izvedenih s strani haktivističnih skupin (1,09%).

Zaskrbljujoč je podatek, da je skoraj v eni petini prišlo izgube podatkov po naključju. Menim, da bi najučinkoviteje zmanjšali tovrstne incidente z vzpostavitvijo celovite varnostne kulture, ne samo v organizacijah temveč tudi v zasebnem življenju državljanov.



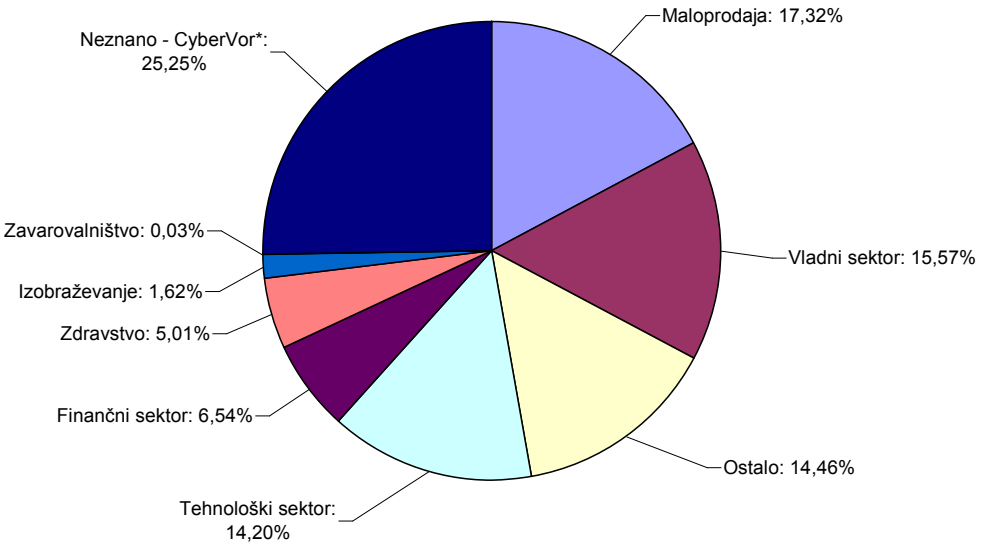
Slika 26: Graf razporeditve virov napadov s posledicami izgube podatkov, celoten svet od leta 2013 do 2016 (vir: BreachLevelIndex.com)

8.4 Posledice incidentov glede na sektor - svet

Pregled statističnih podatkov po deležu izgubljenih ali ukradenih zapisov glede na sektor od leta 2013 do avgusta 2016 pokaže, da je s 17,32% najbolj na udaru maloprodaja. Sledijo podatki vladnega sektorja s 15,57% in tehnološki sektor s 14,2%.

Zanimivo je, da je zdravstveni sektor s 5,01% le malenkost za finančnim sektorjem, ki beleži 6,54% izgubljenih ali ukradenih podatkov. Ostali sektorji skupaj beležijo 14,20% izgubljenih oziroma ukradenih podatkov [61].

Potrebno je pojasniti, kaj na sliki 27 pomeni "Neznano – CyberVor*", ki ima 25,25 odstotni delež. Tu gre za približno 4,5 milijarde zapisov, ki so bili odtujeni iz več kot 420 tisoč spletnih strežnikov in strežnikov FTP (angl. file transfer protocol). Po oceni podjetja HoldSecurity, LLC [97] naj bi šlo za približno 1,2 milijarde enoličnih (angl. unique) avtentikacijskih zapisov (največkrat uporabniško ime in geslo). Ker izvor teh zapisov ni znan, so klasificirani pod oznako neznano. CyberVor ("vor" v ruskem jeziku pomeni tat) pa je ruska kiber kriminalna združba, ki je v letu 2013 pričela svoj kibernetski pohod in ukradla omenjeno število zapisov z namenom nadaljnje uporabe in preprodaje teh zapisov.



Slika 27: Graf s posledicami izgube podatkov glede na sektor, celoten svet od leta 2013 do 2016 (vir: BreachLevelIndex.com)

8.5 Priporočila Sloveniji glede na trende v svetu

8.5.1 Pregled

Podatki SURS [90] o posledicah incidentov iz leta 2010 niso najlažje primerljivi s statističnimi podatki, ki so na voljo za svet. SURS ne vodi ocene števila izgubljenih zapisov, SI-CERT [85] pa pri prijavljenih incidentih ne vodi oziroma ne objavi

velikosti podjetja in sektorja, v katerem podjetje deluje. Na ta način je zelo težko narediti primerjavo med temi podatki.

Glede na pregled statističnih podatkov v svetovnem merilu menim, bi Slovenija morala poleg nekaterih dejavnosti, ki jih je SURS že statistično ocenjeval, dodatno preveriti varnost na naslednjih področjih:

- vladni sektor in javna uprava,
- zdravstvo,
- pravni sektor,
- računovodski sektor,
- izobraževanje.

Na področju finančnega in zavarovalniškega sektorja pa bi bilo potrebno preveriti, kakšen je bil trend posledic incidentov na področju varnosti IKT od leta 2010 do danes.

8.5.2 Vladni sektor in javna uprava

Na podlagi trendov incidentov v svetu menim, da bi morala Slovenija tudi na tem področju opraviti primerno vrednotenje ter poskrbeti predvsem za tehnični pregled uporabljene PO, preverjanje pogodbenih partnerjev in primerno ozaveščanje zaposlenih.

8.5.3 Zdravstvo

Na podlagi statističnih podatkov se na svetovnem nivoju beleži 5% izgub ali zlorab podatkov na področju zdravstva, zato predlagam, da tudi v Sloveniji preverimo kakšno je stanje varnosti na tem področju.

To je dejavnost, ki razpolaga z najobčutljivejšimi osebnimi in drugimi podatki. V slovenskem zdravstvu se uporablja množica sistemov IKT, ki so med seboj večinoma nekompatibilni in nepovezani [53, str. 27], zato je ključnega pomena, v kolikšni meri je bilo poskrbljeno za tehnično varnost in tudi za zavedanje zaposlenega osebja.

8.5.4 Pravni sektor

Predvsem večje, zlasti mednarodne pravne pisarne, razpolagajo z veliko količino zaupnih informacij o drugih organizacijah, njihovih transakcijah, prodajah, prevzemih, pogodbah ipd. Občasno hranijo tudi gesla za dostope do določenih sistemov IKT podjetij za katera delajo oziroma pripravljajo pogodbe ali skrbne preglede (angl. due dilligence). Zaradi tega so takšne pisarne zanimive za zunanje zlonamerneže, ki poskušajo priti do teh informacij in jih prodati ali drugače izkoristiti [84]. Lahko gre tudi za gospodarsko vohunjenje.

Svetovni statistični podatki[23] kažejo trend rasti incidentov v pravnem sektorju, zato je priporočljivo, da podjetja, ki delujejo v navedenih dejavnostih, posvetijo potreben poudarek k izboljšanju varnosti svojih sistemov IKT in izobraževanju zaposlenih na področju organizacijske varnosti.

[23] Na sliki 27 so te dejavnosti zastopane pod oznako "ostalo, 14,46%".

8.5.5 Računovodski sektor

Večji in veliki računovodski servisi, ki skrbijo za veliko število svojih strank, razpolagajo z veliko količino informacij o finančnih transakcijah v teh podjetjih. Prav zato bi morala biti v teh podjetjih varnost na višjem nivoju.

8.5.6 Izobraževanje

Na sliki 27 vidimo, da se z 1,62% posledic izgube podatkov v svetovnem merilu pojavlja tudi dejavnost izobraževanja, zato je priporočljivo, da tudi Slovenija na tem prodročju naredi preventivni korak. Drugi predlog pa je sistematična vpeljava tematike o varnosti na internetu v vzgojno izobraževalni proces, če to še ni bilo narejeno.

8.6 Zakonske smernice in direktive

8.6.1 Strategija slovenske kibernetske varnosti do leta 2020

Evropska agenda za varnost [94] navaja kibernetski kriminal kot eno od treh groženj za evropsko varnost. Z rastjo vsesplošne uporabe IKT se povečuje tudi kibernetski kriminal, ki obsega širok spekter dejavnosti.

Kibernetski kriminal zajema kazniva dejanja, povezana z vdori v zasebnost posameznikov, krajo identitet, pridobivanjem informacij o posameznikih in pravnih osebah z namenom izsiljevanja, spletnimi goljufijami in prevarami, gospodarskim vohunjenjem ipd.

Obenem pa vključuje tudi kazniva dejanja, povezana s poskusi oviranja delovanja interneta, ki zajemajo vse od množičnega pošiljanje neželene e-pošte in izvajanja porazdeljenih ohromitev storitve, do kibernetskega terorizma, ki lahko povzroči motnje v delovanju infrastrukture IKT ter v nekaterih primerih posledično celo ogrozi življenja.

V dokumentu [91] se Slovenija zavezuje, da bo do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov. Ta cilj obsega osem podciljev:

1) okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti;
2) varnost državljanov v kibernetskem prostoru;
3) kibernetska varnost v gospodarstvu;
4) zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore;
5) zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala;
6) razvoj obrambnih kibernetskih zmogljivosti;
7) zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah;
8) krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem.

Verjamem, da bo ta zaveza pripomogla k večji varnosti IKT v organizacijah ter življenjsko pomembni infrastrukturi (vodni viri, električno omrežje). Seveda pa

morajo organizacije predvsem same poskrbeti za varnost na področju IKT ter za vpeljavo varnostnih organizacijskih politik in te politike tudi izvajati.

8.6.2 Nova uredba EU o varstvu osebnih podatkov

Evropski parlament je 14. aprila 2016 letos potrdil Uredbo Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Uredba), ki je pričela veljati 25. maja 2016, njene določbe pa se bodo neposredno uporabljale v vseh državah članicah najkasneje spomladi 2018. Med pomembnimi spremembami, ki jih prinaša nova Uredba, so izpopolnitve uveljavljanja pravic posameznika – določena je na primer obveznost upravljavcev (oseb, odgovornih za obdelavo podatkov), da posameznikom zagotavljajo pregledne in lahko dostopne informacije posameznikom o obdelavi njihovih podatkov. Podrobno so opredeljene tudi splošne obveznosti upravljavcev in oseb, ki osebne podatke obdelujejo v njihovem imenu (obdelovalci).

Zelo pomembni pridobitvi sta obveznost izvajanja ustreznih varnostnih ukrepov in obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov. Poleg tega bodo organizacije v javnem sektorju ter velika podjetja in podjetja, katerih temeljne dejavnosti zajemajo obsežno obdelavo posebnih vrst podatkov**,** morali imenovati uradno (odgovorno) osebo za varstvo podatkov. Obenem Uredba uvaja tudi obveznost poročanja nadzornemu organu (v Sloveniji je to Informacijski pooblaščenec) v primeru kršitve varstva osebnih podatkov. Kršitve zajemajo kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Uredba glede poročanja določa, da mora v primeru kršitve varstva osebnih podatkov vsaka organizacija, ki šteje za upravljavca osebnih podatkov, brez nepotrebnega odlašanja oziroma najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvestiti pristojni nadzorni organ. Če uradno obvestilo nadzornemu organu ni podano v 72 urah, mu je treba priložiti navedbo razlogov za zamudo. V primerih, ko kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, pa mora upravljavec brez nepotrebnega odlašanja o kršitvi varstva osebnih podatkov obvestiti tudi posameznike, na katere se ti osebni podatki nanašajo.

8.6.3 Nova Direktiva EU o varnosti omrežij in informacij

Dne 6. julija 2016 je Evropski parlament sprejel Direktivo 2016/1148 [69] o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Evropski uniji oziroma takoimenovano Direktivo NIS , ki je pričela veljati 8. avgusta 2016. Direktiva bo poenotila nekatere ukrepe držav članic za zaščito informacijskega (danes pogosto rečemo tudi: kibernetskega) okolja, saj je to namreč postalo zelo pomemben del naših življenj. Države članice EU imajo slabi dve leti časa, da vsebino Direktive NIS prenesejo v nacionalne zakonodaje, tako da sprejmejo ustrezno zakondajo, ki bo urejala področje varnosti omrežij in informacijskih sistemov. Direktiva NIS ima namen zagotoviti enotno raven varnosti omrežij in informacijskih sistemov na območju celotne EU, seveda pa lahko posamezne

države članice sprejmejo določbe za doseganje višje stopnje varnosti omrežja in informacijskih sistemov, kot jo določa Direktiva NIS.

Direktiva NIS med drugim od držav članic zahteva, da do maja 2018 zakonsko uredijo naslednja področja [69]:

a) sprejem nacionalne strategije za varnost omrežij in informacijskih sistemov;
b) določitev pristojnih organov za nadzor implementacije določb Direktive NIS;
c) vzpostavitev mreže skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT), ki bi prispevali h krepitvi zaupanja med državami članicami ter spodbudili hitro in učinkovito operativno sodelovanje.

Po končani implementaciji Direktive NIS v slovensko zakonodajo bo za podjetja, ki veljajo za izvajalce bistvenih storitev ali ponudnike digitalnih storitev, veljala obveznost obvladovanja tveganj in poročanja o varnostnih incidentih pristojnim organom. Med ukrepe za obvladovanje tveganj spadajo ukrepi za prepoznavanje tveganj incidentov, preprečevanje in odkrivanje incidentov ter njihovo obvladovanje in ukrepi za ublažitev njihovih učinkov.

Glede na določbe Direktive NIS med izvajalce bistvenih storitev spadajo podjetja, ki zagotavljajo storitve, ki so bistvene za ohranitev ključnih družbenih in/ali gospodarskih dejavnosti, pod pogojem, da je zagotavljanje teh storitev odvisno od omrežij in informacijskih sistemov ter bi tako morebiten incident imel pomemben negativen vpliv na zagotavljanje teh storitev. Ponudniki digitalnih storitev pa v smislu Direktive NIS zajemajo predvsem ponudnike spletnih trgovin, spletnih iskalnikov in storitev računalništva v oblaku.

Sektorji podjetij, ki jih zajema Direktiva NIS, so energetika, promet, bančništvo, finančni sektor, zdravstveni sektor, oskrba s pitno vodo in digitalna infrastruktura.

V skladu z določbami Direktive NIS bodo države članice morale z nacionalno zakonodajo predpisati, da so izvajalci bistvenih storitev in ponudniki digitalnih storitev pristojnemu organu ali skupini CSIRT dolžni brez nepotrebnega odlašanja priglasiti incidente s pomembnim vplivom na neprekinjeno izvajanje storitev, ki jih zagotavljajo, pri čemer mora priglasitev zajemati tudi informacije, na podlagi katerih lahko pristojni organ ali skupina CSIRT določi morebiten čezmejni vpliv incidenta. Pristojni organ ali skupina CSIRT bo lahko po posvetovanju z izvajalcem bistvenih storitev, ki je priglasil incident, o posameznih incidentih obvestila tudi javnost, če je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku.

Prav tako bodo države članice z ustrezno zakonodajo morale zagotoviti, da bodo izvajalci bistvenih storitev ter ponudniki digitalnih storitev določili in sprejeli ustrezne in sorazmerne tehnične ter organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju storitev.

V skladu z določbami Direktive NIS lahko tudi subjekti, ki niso izvajalci bistvenih storitev in tudi ne ponudniki digitalnih storitev, prostovoljno priglasijo incidente, ki imajo pomemben vpliv na neprekinjeno izvajanje storitev, ki jih zagotavljajo.

Menim, da bo Direktiva NIS oziroma na njeni podlagi sprejeta slovenska zakonodaja pripomogla k višji varnosti slovenskih organizacij. Vendar pa bi slovenskim zakonodajnim organom predlagal, da se pri implementaciji Direktive NIS odločijo za strožjo ureditev, v skladu s katero bi bila vsa velika podjetja zavezana poročati pristojnim organom o incidentih, ki so jih zaznali, in ne le podjetja, ki spadajo med izvajalce bistvenih storitev oziroma ponudnike digitalnih storitev, kot to določa novosprejeta Direktiva NIS.

9 Sklepne ugotovitve

V pričujoči magistrski nalogi sem najprej predstavil osnovne pojme in definicije ter ključno družino standardov ISO/IEC 27000 na področju obvladovanja varnosti IKT. Sledila je obravnava obvladovanja neprekinjenega poslovanja (standard ISO/IEC 22301:2012) in načrta obvladovanja obnove po škodnem dogodku s pripadajočim standardom ISO/IEC 24762:2008. Edina stalnica v poslovanju organizacij so spremembe, zato sem predstavil standarde in metodologije na področju obvladovanja sprememb. V desetih smernicah sem zapisal predlog za uspešno obvladovanje sprememb.

Pri preučevanju standardov sem opazil, da slovenski prevodi standardov terminološko ne ustrezajo vedno najbolje smernicam slovenskega knjižnega jezika.

Pomembno se je zavedati, da samo varnostne politike ne bodo rešile varnostnih težav v sistemih IKT, če jih ne bodo izvajali in izboljševali ljudje. V vseh omenjenih procesih kot tudi za uspešno poslovanje podjetja je pomembna pozitivna organizacijska kultura. Kultura organizacijske varnosti je še korak višje. V šestih točkah sem po Trčku in Likarju povzel in predlagal metodo MIS^2 kot vodilo za sistematičen način vzpostavitve varnostne organizacijske kulture.

V nadaljevanju sem predstavil pregled dostopnih statističnih podatkov za slovenska podetja. Namen je bil prikazati, kakšna je slika na področju varnosti IKT glede na velikost podjetja. Naredil sem pregled posledic incidentov glede na velikost in glede na SKD podjetij. Pri pregledu statističnih podatkov sem ugotovil, da so na nekaterih mestih nepopolni ali zaupni. Prav tako bi za bodoče raziskave svetoval upoštevanje nekaterih smernic iz četrtega poglavja, ki bi omogočile podrobnejše analize in primerjave podatkov.

Posebno pozornost sem dal podjetjem, ki delujejo v finančnem sektorju, kajti zaradi svoje narave so navadno zelo na udaru na področju varnsti IKT. Zapisal sem smernice, ki naj bi jih upoštevala podjetja, ki delujejo v finančnem sektorju.

Na osnovi korelacije med posledicami incidentov ter uporabo odprtokodne PO sem glede na velikost podjetij (mala, srednja, velika) skušal najti povezavo med

določenimi posledicami incidentov ter uporabo določene odprtokodne PO. Z bolj podrobnimi podatki (uporaba licenčne programske opreme), bi morda lahko prišel do kakšnega bolj natančnega sklepa.

Z analizo statističnih podatkov SURS, baze NVD CVE in orodja CVE-analyzer sem ugotovil, da so bila v letu 2011 slovenska podjetja, ki so uporabljala odprtokodne spletne brskalnike bolj ranljiva od slovenskih podjetij, ki so uporabljala zgolj licenčni brskalnik Microsoft Internet Explorer. Moram priznati, da sem kot ljubitelj odprtokodnega brskalnika Mozilla Firefox pričakoval drugačne rezultate. Glede na predstavljene postopke in ugotovitve bi bilo zanimivo opraviti nadaljnje analize in primerjave tudi za ostale tipe programske opreme.

V šestem poglavju sem naredil analizo statističnih podatkov o uporabi prenosnih naprav v slovenskih podjetjih v letu 2012. Podal sem dobre prakse in ključne točke za obvladovanje prenosnih naprav v poslovnem okolju.

Sedmo poglavje podaja ključne procese in standarde, ki jih organizacije lahko uporabijo v procesu razvoja PO. Poleg tega sem zbral najpogostejše napake, ki se pojavijo pri razvoju ter smernice za razvoj varnih aplikacij. Glede na število mobilnih aplikacij, ki se pojavljajo kot gobe po dežju bi bilo zanimivo podrobneje pregledati tudi stanje na tem področju.

V osmem poglavju sem podal še dodatna priporočila na področju uporabe lahkih metodologij, družbenih omrežij, IT v senci in računalništva v oblaku. Naredil sem hiter pregled posledic incidentov s posledico izgube ali kraje zapisov v svetovnem merilu. Najpogosteje je vir takšnega incidenta zunanji napadalec. Zanimivo je tudi to, da je skoraj trikrat več incidentov izvedenih po naročilu državnih organov kot pa s strani haktivističnih skupin. Pregled posledic incidentov glede na sektor kaže, da je najbolj ranljiv maloprodajni sektor, ki mu glede na delež izgubljenih ali ukradenih zapisov tesno sledi vladni sektor. Predlagam analizo stanja in preventivne ukrepe za izboljšanje varnosti IKT na področju vladnega sektorja, javne uprave, zdravstva, pravnega, računovodskega sektorja in izobraževanja.

V tej nalogi so zbrani ključni standardi, metodologije in smernice za obvladovanje varnosti IKT v organizacijah ne glede na njihovo velikost. Za vsako organizacijo pa je zelo pomembno, da učinkovito vpelje kulturo organizacijske varnosti.

Zaključujem z mislijo, ki jo je Bruce Schneier zapisal leta 2004 [46]: "Kdor misli, da lahko tehnologija reši varnostne probleme, potem ne razume niti problemov, niti tehnologije."

10 Priloge

10.1 Priloga 1

V nadaljevanju sledi opis orodja CVE-analyzer, ki sem ga razvil za potrebe analiz v petem poglavju te magisterske naloge.

CVE-analyzer 1.1

Navodila za namestitev in uporabo

CVE-analyzer je sklop modularnih orodij za oceno ranljivosti realnih sistemov IT (strojna in programska oprema) na osnovi podatkov iz baze ranljivosti MITRE CVE. Takšno orodje je lahko v pomoč organizacijam pri ocenjevanju njihove dejanske ranljivosti IKT, glede na to, da imajo znan nabor programske opreme. Pomaga jim lahko pri odločitvah o nadgradnjah sistemov ali menjavi dela programske opreme, pri čemer lahko organizacije vnaprej določijo predvideno stopnjo ranljivosti nadgrajenih sistemov. To je najbolj pogost primer za oceno ranljivosti posameznega sistema. Ocenjujejo lahko namreč točno določeno, nameščeno ali predvideno programsko opremo za namestitev.

Takšen nabor programske opreme je lahko npr. dejanska programska oprema na strežniku ali delovni postaji. Primera v tabeli 43 kažeta, kako narediti primerjavo ranljivosti med ekvivalentnima sistemoma (odprtokodni, licenčni), pri čemer nas zanima, kateri sistem je bolj varen glede na znane ranljivosti CVE programske opreme (PO).

DELOVNA POSTAJA	ODPRTOKODNI (O)	LICENČNI (L)
Operacijski sistem	Cent OS 5.4 (32-bit) (Linux kernel 2.6.18.1)	Windows XP Professional sp3 (32-bit)
Spletni brskalnik	Mozilla Firefox 3.5.6	Internet Explorer 8
Program za e-pošto	Mozilla Thunderbird 3.0	MS Outlook 2007 sp2
Pisarniška programska oprema	Open Office 3.1.1	MS Office 2007 sp2
PDF reader	Evince 0.6	Adobe Acrobat Reader 9.0
Multimedia	VLC Media Player 1.0.3	Windows Media Player 11
	Adobe Flash Player (10.0.12.36)	Adobe Flash Player (10.0.12.36)
Programi za delo s slikami	GIMP 2.6.11	Adobe Photoshop CS4 (v11)

Tabela 43: Izbor potencialne programske opreme za delovno postajo (DP), leto 2010

Na osnovi tako zastavljenih naborov PO lahko enostavno delamo primerjave ranljivosti. Lahko na primer zamenjamo del PO z neko drugo, podobno kot bi zlagali lego-kocke, in iščemo najboljšo kombinacijo glede na potrebe in zmožnosti organizacije.

Primer dileme oddelka IT v velikem slovenskem podjetju na področju turizma:

- Kakšna bo stopnja ranljivosti glede na obstoječi strežniški sistem, če zamenjamo operacijski sistem iz CentOS 7 x64 (Linux) z licenčnim operacijskim sistemom Windows server 2012 x64?
- Ali bo stopnja ranljivosti v primeru zamenjave nižja ali višja ter kolikšna bo razlika?

S CVE-analyzerjem lahko organizacije hitro in enostavno dobijo odgovor na tovrstna vprašanja. Podobnejša analizira dveh primerov primer sledi v tabelah 44 in 45.

CVE-analyzer je sicer napisan tako, da ga nekdo z minimalnim znanjem SQL in programskega jezika PHP lahko nadgradi oziroma spremeni njegovo delovanje glede na specifične potrebe.

V osnovi pa to niti ni potrebno. Večina nastavitev se namreč nastavlja in kombinira v tekstovnih nastavitvenih datotekah, ki jih skripte .php uporabijo za izvedbo postopkov analize. Te datoteke so naslednje:

a) "./templates/*.sql" - sql z uporabo "placeholderjev/replacerjev";
b) "./templates/*.agr" - tekstualna datoteka, kjer s posebnimi pravili določamo izbor, vrstni red ter agregacijo polj za izvoz v poročilo oblike CSV;
c) "./data/cpe/*.cfg" - konfiguracija po sekcijah. S kombinacijo teh datotek določamo kriterije analize za izbrano PO.

Primer konfiguracije za posamezno PO:

```
"./data/cpe/01 Windows XP Professional sp3 (32-bit).cfg"

[TITLE]
01) Windows XP Professional sp3 (32-bit)
[CPE]
cpe:/o:microsoft:windows_xp::sp3
cpe:/o:microsoft:windows_xp:-:sp3
cpe:/o:microsoft:windows_xp::sp3:x86
cpe:/o:microsoft:windows_xp:sp3
cpe:/o:microsoft:windows_xp:sp3:unknown:english
cpe:/o:microsoft:windows_xp:unknown:sp3
[SUMMARY SEARCH]
%windows%%xp%%sp3%
```

Primer konfiguracije za agregacijo izpisa CVE:

```
"./templates/cpe-report-template.agr"
[HEADER NAMES]
product;vulns;cvss score (sum);cvss score (avg);
access vector: NETWORK;availability impact: COMPLETE;

[FIELD AGGREGATION]
title:group by;title:count;cvss_score:sum;cvss_score:avg;
cvss_access_vector:count:NETWORK;cvss_availability_impact:cou
nt:COMPLETE;
```

```
# comments and explanation of commands #
#              Control              names              Format:
field_name:aggregation_command[:aggregation_value]
# Possible aggregation commands:
#  group by (field name of wich to get rows/values for
aggregation; must be set in WHERE clause)
# count (counts rows)
# avg (average of values)
# sum (sum of values)

# aggregation_value = actual value in
# this field we want to aggregate by
```

1. Namestitev CVE-analyzerja:

1) Razširite "CVE-analyzer-v1.1.zip" v neko mapo "BASE_PATH" na računalniku.
2) Na sistemu potrebujete delujočo bazo MySQL 5.0. ali novejšo različico ter PHP 5.3 ali novejšo različico. Potrebni (angl. required) paketi: mysql, php, php-mysql, php-xml. Priporočljivo je, da je PHP interpreter dostopen preko sistemske spremenljivke PATH, da ga je možno zagnati preko ukazne lupine (shell).
3) S skrbniškimi pravicami se povežite na podatkovni strežnik MySQL in ustvarite novo shemo (cvedb), uporabnika (cveuser) ter geslo (cvedb) za tega uporabnika.
4) S pomočjo datoteke "./install/cve-db-create-structure.sql" ustvarite strukturo baze cvedb.
5) Pred začetkom dela s skriptami PHP morate v datoteki "./include/settings.php" nastaviti pravilno pot do strukture datotek "BASE_PATH" CVE-analyzer (glejte komentarje v settings.php).
6) Iz spletne strani https://nvd.nist.gov/download.aspx prenesite seznam ranljivosti za željeno obdobje, na primer "https://nvd.nist.gov/feeds/xml/cve/nvdcve-2.0-2010.xml.zip"[24] [25] [26]. Shranite jo v mapo "./data" ter jo z ukazom "./import-nvdcve.php nvdcve-2.0-2010.xml" uvozite v bazo. Zdaj je podatkovna baza za leto 2010 pripravljena za nadaljnjo analizo.
7) Za obdelavo CSV oblike poročil boste potrebovali program za tabelarično obdelavo (Microsoft Excel, Open Office Calc, Libre Office Calc ali podobnega).
8) Predloge v mapi "./templates" določajo osnovno delovanje ogrodja (SQL select, CSV izvoz, ...). S spremembami teh predlog spremenimo izpise ali prilagodimo ogrodje za delo z novejšo različico baze NVD CVE. Z minimalnimi spremembami v programski kodi in v predlogah lahko

[24] CVE-analyzer je bil ustvarjen in testiran na nvdcve-2.0-XXXX.xml.zip. Na tej osnovi je bil CVE-analyzer razvit zaradi potrebe po primerjavi ranljivosti CVE s statistikami slovenskega statističnega urada - SURS o varnosti odprtokodne PO v letu 2011, kajti za 2012-2016 takšni statistični podatki na SURS ne obstajajo.
[25] Datoteka "nvdcve-2.0.xml" je format CVE baze, ki ima dodan CVSS scoring in CPE ranljivih konfiguracij (angl. vulnerable-configuration) PO in ranljive PO (angl. vulnerable software list).
[26] Vsi možni viri za uvoz CVE so dostopni na naslovu: https://nvd.nist.gov/download.aspx.

uporabimo ogrodje za kakšen podoben problem, ki uporablja bazo podatkov MySQL. Na ta način enostavno izvedemo analizo ter zapis rezultatov v tabelo za nadaljnje agregiranje ter seveda agregacijo in izvoz podatkov v CSV datoteko.

9) Vse napake in izpisi ogrodja se vršijo v dnevniško (log) datoteko, katere pot nastavite v "./include/settings.php" s parametrom "ERROR_LOG".

2. Postopek analize:

1) Identificirajte (CPE) programske proizvode na sistemih, za katere potrebujete oceno ranljivosti glede na bazo CVE. Pomagajte si s slovarjem proizvodov (Official Common Platform Enumeration (CPE) Dictionary). Dostopen je na spletnem naslovu: https://nvd.nist.gov/cpe.cfm.
2) Za posamezni izbor (konfiguracijo) PO ustvarite v mapi "./data/cpe/*.cfg" svojo konfiguracijsko datoteko. Poimenovanje datoteke ni pomembno, je le za vašo evidenco. Pomembne so nastavitve v tej datoteki. Te vplivajo na analizo in izvoz v CSV. Za podrobnejša navodila o nastavitvah si poglejte komentarje v "./data/cpe/manual/product-config_template.cfg". Če želite za lažjo primerjavo različnih izborov PO obdržati isti vrstni red izpisov, lahko dodate številko kot vrstni red na začetek imena PO (sekcija [TITLE]) v .cfg datoteki. Ta številka bo potem po abecednem redu določala vrstni red izpisa. Na primer: "01) Apache server 2.2.3".
3) Zaženite `"./cpe-scoring.php"`. Programska skripta iz mape "./data/cpe/*.cfg" prebere vse *.cfg datoteke in naredi analizo, ki jo zapiše v podatkovno bazo, tabela "tmp_analysed_cpes". Naprednejši uporabnik lahko potem z SQL orodji naredi dodatno analizo ali popravke. Rezultati v tej tabeli namreč prav zaradi tega še niso agregirani.

   Parametri, ki jih upošteva skripta:
   a) --CVE-YEAR-min: najstarejši uporabljeni zapisi CVE glede na leto objave;
   b) --CVE-YEAR-max: uporabi zapise CVE do vključno tega leta;
   c) --CSV-EXPORT: ime izhodne CSV datoteke. Če ta parameter ni določen, je potrebno izpis narediti posebej, kot je razloženo v koraku 3.

   Primer klica, ki naredi analizo za ./data/cpe/*.cfg ter pri tem upošteva vse zapise CVE med letoma (vključno z) 2002 do 2016.
   ```
   cpe-scoring.php --CVE-YEAR-min=2002 --CVE-YEAR-max=2016
   ```

   Če imate pripravljenih več različnih konfiguracij PO, jih lahko shranite oziroma prestavite v podmape. Za analizo ter izvoz v aktualno CSV datoteko šteje le to, kar je nastavljeno v konfiguracijskih datotekah na lokaciji "./data/cpe/*.cfg". Na ta način lahko enostavno kombinirate sezname različne PO v konfiguracijah za analizo.

3. Izvoz agregiranih rezultatov v CSV

Izvoz agregiranih rezultatov opravite s "./cpe-export-csv.php". Tudi izvoz je modularno pisan tako, da ga nekdo z minimalnim znanjem PHP lahko hitro prilagodi, vendar za različne agregacije izvoza to ni potrebno, saj se tudi te

nastavljajo v že omenjeni mapi "./templates" v datoteki "cpe-report-template.cfg". V nastavitvah določite polja, vrstni red polj za izpis, glavo csv datoteke ipd. Pravila za agregacijo polj je možno nastavljati z naslednjimi agregatorji: group by, count, sum, avg in še po ročno določenih kriterijih (vrednosti posameznih polj). Za podrobnejša pojasnila poglejte komentarje v datoteki
"./templates/cpe-report-template.cfg".

Izvoz izvršite tako, da izvedete ukaz:
```
./cpe-export-csv.php name-of-report.csv
```

Nadaljujte s korakom številka 5.

4. Združitev 2. in 3. koraka ter avtomatizacija izvoza v CSV
V primeru, da ob zagonu "cpe-scoring.php" določite tudi parameter izhodne datoteke "--CSV-EXPORT", skripta cpe-scoring.php avtomatsko naredi tudi izvoz v CSV.

Primer klica, ki naredi analizo za nastavljene proizvode v datotekah "./data/cpe/*.cfg" ter pri tem upošteva vse CVE zapise med letoma (vključno) z 2015 do 2016.
```
./cpe-scoring.php --CVE-YEAR-min=2015 --CVE-YEAR-max=2016
--csv-export=sistemi-ocena-2015-2016.csv
```

4. a) Kadar želite narediti analizo CVE ranljivosti, kjer je "--CVE-YEAR-min" leto fiksno določeno, in želite določiti agregirano število ranljivosti po posamezni CPE oznaki med določenimi časovnimi obdobji, smiselno prilagodite in uporabite skripto "./multi-year-cpe.sh".

Ta skripta sprejme le en parameter, ki je osnovno ime (angl. basename) izhodnih poročilnih CSV datotek.

Primer klica:
```
multi-year-cpe.sh osnovno-poimenovanje
```
vrne rezultate v več datotekah v podobni strukturi kot je tale:
```
osnovno-poimenovanje_2002-2003.csv
osnovno-poimenovanje_2002-2004.csv
osnovno-poimenovanje_2002-2005.csv
...
osnovno-poimenovanje_2002-2016.csv
```

4. b) Kadar potrebujete ločena poročila za določeno CPE konfiguracijo po posameznih letih, lahko uporabite skripto "multi-year-cpe-1-year-step.sh".

```
./multi-year-cpe-1-year-step.sh sistemi-ocena
```
generira podobno strukturo poročil:
```
sistemi-ocena-2002-2002.csv
sistemi-ocena-2003-2003.csv
sistemi-ocena-2004-2005.csv
```

```
...
sistemi-ocena-2016-2016.csv
```

5. Nadaljnja analiza in oblikovanje

Datoteka s poročilom se bo po uspešnem agregiranju pojavila v mapi "./data/cpe" pod imenom, ki ste ga določili. Z različnimi nabori CPE .cfg datotek lahko ustvarite poljubno število konfiguracij PO za medsebojno primerjanje in nadaljnjo obdelavo izvozov .CSV v tabelaričnih programih omenjenih v razdelku 1.7). Ko imate potrebne .CSV izvoze, jih lahko med sabo poljubno primerjate in iz njih na enostaven način pridobite ocene o ranljivosti (glede na CVE) posameznih naborov PO.

Opomba: če za nek izbran nabor CPE (.cfg datoteka) ni najdene nobene ranljivosti, se ta CPE ne pojavi med izpisi v CSV poročilu.

Primer agregiranih izpisov analize za tabelo 43 sledi v tabelah 44 in 45. Na ta način lahko enostavno obdelujete in primerjate agregirane podatke iz CVE.

Opomba:

Izpisi v tabelah 44 in 45 so narejeni na osnovi posnetka CVE znanih ranljivosti iz leta 2010[27]. To pomeni, da so bile analizirane le znane ranljivosti v izbranem časovnem obdobju, pri čemer lahko obstaja tudi več ranljivosti za posamezen proizvod, ki v tem obdobju še niso bile znane oziroma zavedene v bazo CVE. To predpostavko lahko enostavno preverimo in v podatkovno bazo uvozimo še znane ranljivosti za ostala leta (2011-2016). Ob ponovni analizi tako lahko dobimo bolj natančno sliko dejansko znanih ranljivosti določenih proizvodov skozi čas.

Proizvod	Število ranljivosti	Točke CVSS (vsota)	Točke CVSS (povprečje)	Pristopni vektor: OMREŽJE	Vpliv na razpoložljivost sistema: POPOLN
CentOS 5.4 (Linux Kernel 2.6.18 x64)	123	603	4,9	20	76
Mozilla Firefox 3.5.6	**80**	**593,5**	**7,42**	78	48
Mozilla Thunderbird 3.0	53	416,4	7,86	51	37
Open Office 3.1.1	10	90,6	9,06	9	10
Evince 0.6	4	30,4	7,6	4	4
VLC Media Player 1.0.3	10	77,2	7,72	10	4
Adobe Flash Player for Linux (10.0.12.36)	5	41,5	8,3	5	4
GIMP 2.6.11	4	30,4	7,6	4	1
Vsota:	289	1883	7,56*[28]	181	184

Tabela 44: Agregirane vrednosti ocene ranljivosti po CVE za izbor odprtokodne PO iz tabele 43

[27] https://nvd.nist.gov/feeds/xml/cve/nvdcve-2.0-2010.xml.zip

[28] Skupno povprečje (avg) ocene CVSS SCORE*

Proizvod	Število ranljivosti	Točke CVSS (vsota)	Točke CVSS (povprečje)	Pristopni vektor: OMREŽJE	Vpliv na razpoložljivost sistema: POPOLN
Windows XP Professional sp3 (32-bit)	110	868,7	7,9	73	98
Internet Explorer 8	**46**	**336,5**	**7,32**	46	28
MS Outlook 2007 sp2	3	25,4	8,47	3	2
MS Office 2007 sp2	30	258,8	8,63	30	26
Adobe Acrobat Reader 9.0	58	519,4	8,96	58	53
Windows Media Player 11	3	17,9	5,97	3	1
Adobe Flash Player (10.0.12.36)	55	489	8,89	55	50
Adobe Photoshop CS4 v11	2	18,6	9,3	2	2
Vsota:	307	2534,3	8,18*	270	260

Tabela 45: Agregirane vrednosti ocene ranljivosti po CVE za izbor licenčne PO iz tabele 43.

Iz podatkov analize v tabeli 45 lahko vidimo, da ima odprtokodni brskalnik "Mozilla Firefox 3.5.6" v primerjavi z licenčnim brskalnikom Microsoft Internet 8 (IE8) skoraj dvakrat višje število ranljivosti. Podobno velja za težo ranljivosti v točkah CVSS.

Po enačbi (5.1) lahko izračunamo relativni razliki takole:

$$d_r(\text{stRanljivosti\_Firefox356}; \text{stRanljivosti\_IE8}) = d_r(80; 46) = 54\% \quad (10.1)$$

$$d_r(\text{stTockCVSS\_Firefox356}; \text{stTockCVSS\_IE8}) = d_r(593{,}5;\ 336{,}5) = 55\% \quad (10.2)$$

Ugotovimo, da je glede na podano analizo odprtokodni brskalnik Mozilla Firefox 3.6.5 po številu ranljivosti za 54% ranljivejši od licenčnega Internet Explorerja 8 (10.1). Teža ranljivosti pa je za en procent (55%) višja.

Na podoben način lahko ocenjujemo in med seboj primerjamo PO glede na oceno znanih ranljivosti v bazi NVD CVE.

Literatura

Znanstvena literatura

[1] BOEHM, Barry, and Hoh In.: "Aids for identifying conflicts among quality requirements." IEEE Software 13.2 (1996): 25-35.

[2] COPELAND, Wes; CHIANG, Chia-Chu: “Securing Enterprise Mobile Information”, 2012 International Symposium on Computer, Consumer and Control, 2012 IEEE, zvezek 30, str 80 – 83.

[3] EPSTEIN, Jeremy: "Security lessons learned from Société Générale." IEEE Security & Privacy 3.6 (2008): 80-82.

[4] GUO, Minzhe; WANG, Ju An: “An Ontology-based Approach to Model Common Vulnerabilities and Exposures in Information Security”, 2009 ASEE Southeast Section Conference, 10 str.

[5] KHALIL, Issa M., Abdallah Khreishah, and Muhammad Azeem: "Cloud computing security: a survey", Computers 3.1 (2014): 1-35.

[6] KRAJNC, Tomaž: Upravljanje sprememb IT storitev, 25. Mednarodna konferenca o razvoju organizacijskih znanosti - MANAGEMENT SPREMEMB; 15. - 17. marec 2006, Portorož, Slovenija.

[7] LALA, Jaynarayan H.; SCHNEIDER, Fred B.: "It monoculture security risks and defenses." IEEE Security & Privacy 7.1 (2009): 12-13.

[8] LEACH, John: "Improving User Security Behavior". Computers & Security, Vol. 22, No. 8, pp. 685-692, Elsevier, (2003).

[9] MALCOLMSON, Jo: “What is Security Culture? Does it differ in content from general Organisational Culture?”, Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on, str. 361 - 366.

[10] NEUHAU, Stephan; ZIMMERMANN, Thomas: "Security Trend Analysis with CVE Topic Models", University of Calgary, Technical Report 2010-970-19, 13-Aug-2010, 15 strani.

[11] NUNES, F. J. B.; BELCHIOR, A. D.; ALBUQUERQUE, A. B.: “Security Engineering Approach to Support Software Security”, 2010 IEEE 6th World Congress on Services, Services (SERVICES-1), str. 48-55.

[12] SANDERS, A.; Tong Sun; Yin Pan; Bo Yuan: "Correlating Risk Findings to Quantify Risk": Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom), str. 752-759.

[13] SILIC, Mario, BACK, Andrea: "Shadow IT – A view from behind the curtain", University of St. Gallen, Switzerland, junij 2014.

[14] YUAN, Ding, et al.: "Simple testing can prevent most critical failures: An analysis of production failures in distributed data-intensive systems.", 11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14), 2014.

[15] WILLIAMS, G.P.: “Cost effective assessment of the infrastructure security posture”, 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012.

[16] TRČEK, Denis; LIKAR, Borut: "Information Systems Security Management By Deployment of Innovations Management Techniques", Latest Trends in Applied Computational Science, ISBN: 978-1-61804-171-5, str: 21 - 24.

[17] TRČEK, Denis: "Managing Information Systems Security and Privacy"; Springer Verlag; 5.12.2006, 236 strani.

[18] SU-HYUN, Kim and IM-YEONG Lee: “Study on User Authority Management for Safe Data Protection in Cloud Computing Environments”, Symmetry 2015, 7, 269-283; ISSN 2073-8994.

Ostala literatura

[19] ALBERTS, C. et al.: "OCTAVE - The Operationally Critical Threat, Asset, and Vulnerability Evaluation", Carnegie Mellon - Software Engineering Institute, december 2001. Dostopno na: www.cert.org/octave.

[20] AGUIRRE, DeAnne, ALPERN, Micah: "10 Principles of Leading Change Management"; Organizations & People, Summer 2014 / Issue 75, June 6, 2014. Dostopno na: http://www.strategy-business.com/article/00255.

[21] ANSI/IEEE recommended practice for software design descriptions, IEEE Std 1016-1998, http://www.ieee.org.

[22] CAMERON, Esther; GREEN, Mike: "Making sense of change management: a complete guide to the models, tools and techniques of organizational change", Kogan Page Publishers, 2015.

[23] CARNALL, Colin A.: "Managing change in organizations", Pearson Education, 2007.

[24] FAIRLEY, R.: "Software Engineering Concepts", New York, McGraw-Hill, 1985.

[25] HOWARD, M.; D. LeBlanc: "Writing Secure Code 2ndEd", Redmond, WA: Microsoft (2003).

[26] HVALA D.: "Projekt? Brez panike!", Revija Monitor - priloga Sistem; Ljubljana, september 2003, str. 12-15.

[27] IEEE Std 830-1998; IEEE Computer Society. Software Engineering Standards Committee and IEEE-SA Standards Board, 1998. IEEE recommended practice for software requirements specifications. Institute of Electrical and Electronics Engineers, 25.6.1998; 37 strani.

[28] ISO/IEC 9001:2015 - Quality management systems - Requirements. ISO/IEC, Geneve 2015.

[29] ISO/IEC 15408-1 - Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model, 2005.

[30] ISO/IEC 15408-2 - Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements, 2005.

[31] ISO/IEC 15408-3 - Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements, 2005.

[32] ISO/IEC 20000-1:2011 - Information technology -- Service management -- Part 1: Service management system requirements, Geneve 2011.

[33] ISO/IEC 20000-2:2012 - Information technology -- Service management -- Part 2: Guidance on the application of service management systems, Geneve 2012.

[34] ISO/IEC 21827:2008 - Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)

[35] ISO/IEC 22301:2012 - Societal security -- Business continuity management systems, 34 strani. ISO/IEC, Geneve 2012.

[36] ISO/IEC 24762:2008 - Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services. ISO/IEC, Geneve 2008.

[37] ISO/IEC 27000:2014 - Information technology -- Security techniques -- Information security management systems – Overview and vocabulary. ISO/IEC, Geneve 2014.

[38] ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements. ISO/IEC, Geneve 2013.

[39] ISO/IEC 27001:2005. Mednarodni standard ISO/IEC 27001 Informacijska tehnologija. Slovenska izdaja, Ženeva 2005.

[40] ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls, 80 strani. ISO/IEC, Geneve 2013.

[41] JESENKO, dr. Jože, ŠIFRER, Jerneja: "Statistika – zbirka rešenih nalog"; Univerza v Mariboru, Fakulteta za varnostne vede, Tipografija d.o.o., Ljubljana 2008.

[42] MAURYA, Ash; REISS, Eric, "Running Lean - How to Iterate from Plan A to a Plan that Works", Second Edition, O'Reilly, 2012.

[43] PHILLIPS, Dwayne: Software Project Manager's Handbook, Principles that work at work. IEEE CS Press, Wiley Interscience, 2. edition, 2004, 504 strani.

[44] RANČIGAJ, Katja in LOBNIKAR, Marko: "Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture", 2012, Maribor: Univerza v Mariboru, Fakulteta za varnostne vede.

[45] ROVERS, Mart: ISO/IEC 20000-1:2011 - A Pocket Guide; Van Haren Publishing, Zaltbommel, 2012.

[46] SCHNEIER, Bruce: "Secrets and lies: digital security in a networked world", John Wiley & Sons, 2011.

[47] SNEDAKER, Susan; RIMA, Chris: "Business continuity and disaster recovery planning for IT professionals", Amsterdam : Elsevier, 2014 2nd ed.

[48] SOLINA, Franc: Projektno vodenje razvoja programske opreme. Založba FE in FRI, Ljubljana 1997, 213 strani.

[49] STIENNON, Richard: "Categorizing Data Breach Severity with a Breach Level Index"; Founder, IT – Harvest, 2013. Dostopno na: http://breachlevelindex.com/pdf/Breach-Level-Index-WP.pdf.

[50] ŠINIGOJ, Aleksander: "Razvoj metode upravljanja tveganj, povezanih z informacijskimi sredstvi v podjetjih", doktorska disertacija, 2008, Univ. Ljubljana, Ekonomska fak.

[51] TITTEL, Ed: "7 Enterprise Mobile Security Best Practices", februar 2014. Dostopno na: http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html.

[52] UTTAL, Bro. "The corporate culture vultures", Fortune 108.8 (1983): 66-72.

[53] VONČINA SLAVEC, Smiljana: "Potrebe ministrstva za zdravje so samo vrh ledene gore, ki predstavlja celotni zdravstveni sistem"; intervju, Varnostni forum 11, letnik IV / 2008, izdaja Palsit d.o.o., Šempeter.

[54] WEINBERG, Gerald M.: Quality Software Management: Vol. 2, First Order Measurment. Dorset House Publishing, New York, 1993.

[55] WENNING, Carl J.: "Percent Difference and Percent Error - Student Laboratory Handbook"; North Carolina State University, avgust 2008. Dostopno na: http://www2.phy.ilstu.edu/~wenning/slh/.

[56] WOOD, Alyssa: "IT in the gutter with mobile compliance", Januar 2016. Dostopno na: http://searchmobilecomputing.techtarget.com/news/4500270274/IT-in-the-gutter-with-mobile-compliance.

Ostali viri

[57] A Complete Guide to the Common Vulnerability Scoring System Version 2.0. Dostopno na: https://www.first.org/cvss/v2/guide.

[58] Alliance for Telecommunications Industry Solutions: ATIS Telecom Glossary 2016. Dostopno na: http://www.atis.org/glossary/definition.aspx.

[59] Android for Work, https://www.android.com/work/

[60] Apache Shiro is a powerful and easy-to-use Java security framework that performs authentication, authorization, cryptography, and session management. Dostopno na: http://shiro.apache.org/

[61] Breach Level Index. Podatki pridobljeni 14.08.2016. Dostopno na: http://breachlevelindex.com

[62] Browser Statistics. Dostopno na: http://www.w3schools.com/browsers/

[63] CAPEC (Common Attack Pattern and Classification). Dostopno na: https://capec.mitre.org/.

[64] Chi-Square Test. Dostopno na: http://www2.lv.psu.edu/jxm57/irp/chisquar.html.

[65] Common Vulnerabilities and Exposures (The Standard for Information Security Vulnerability Names). Dostopno na: http://cve.mitre.org/.

[66] CVE - Common Vulnerabilities and Exposures. Dostopno na: https://cve.mitre.org/.

[67] CVE-Compatible Products and Services. Dostopno na: https://cve.mitre.org/compatible/compatible.html.

[68] CWE - Common Weakness Enumeration. Dostopno na: http://cwe.mitre.org.

[69] DIREKTIVA (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Dostopno na: http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[70] Dropbox – storitev hranjenja in izmenjave datotek v oblaku. Dostopno na: https://www.dropbox.com/.

[71] Firefox release history. Dostopno na: https://en.wikipedia.org/wiki/Firefox_release_history.

[72] Google Chrome release history. Dostopno na: https://en.wikipedia.org/wiki/Google_Chrome_release_history.

[73] Internet Explorer versions. Dostopno na: https://en.wikipedia.org/wiki/Internet_Explorer_versions.

[74] ITIL – A guide to change management. Dostopno na: https://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/servicetransition/chanage_management/ITIL_a%20guide%20to%20change%20management%20pdf.ashx.

[75] KERSNIK, prim. prof. dr. Janko: "Teza – sporočilo raziskovalnega dela, raziskovalno vprašanje - Znanstvenoraziskovalno delo", prosojnice s predavanja "Zdravstveni sistemi v Evropski skupnosti", 31.3.2014. Dostopno na: http://m.mf.uni-lj.si/media-library/2014/08/344617b9e0a7b06cd53d499a32cfc494.pdf

[76] ISO 27001 security - Change management and Control Policy. Dostopno na: http://www.iso27001security.com/ISO27k_Model_policy_on_change_management_and_control.docx.

[77] Minitab. Dostopno na: http://www.minitab.com/en-us/.

[78] National Vulnerability Database (NVD). Dostopno na: https://nvd.nist.gov.

[79] OVAL. Dostopno na: http://oval.mitre.org/.

[80] OWASP (The Open Web Application Security Project) Top 10 – 2013: The ten most critical web application security risks. Dostopno na: https://owasptop10.googlecode.com/files/OWASP Top 10 - 2013.pdf, https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet.

[81] Port80's 2010 - Top 1000 Corporation Web Servers. Dostopno na: https://www.port80software.com/surveys/top1000webservers.

[82] Relative change and difference. Dostopno na: https://en.wikipedia.org/wiki/Relative_change_and_difference.

[83] Samsung KNOX. Dostopno na: https://www.samsungknox.com/en/products/knox-premium.

[84] Security safe: How law firms are facing the growing threat. Dostopno na: https://www.totumpartners.com/printpdf/502.

[85] SI CERT – Poročilo o omrežni varnosti za leto 2015. Dostopno na: https://www.cert.si/.

[86] Six Sigma. Dostopno na: https://en.wikipedia.org/wiki/Six_Sigma.

[87] Sophos Mobile Control. Dostopno na: https://www.sophos.com/en-us/products/mobile-control.aspx.

[88] Spearman's Rank-Order Correlation using SPSS Statistics. Dostopno na: https://statistics.laerd.com/spss-tutorials/spearmans-rank-order-correlation-using-spss-statistics.php.

[89] Standardna klasifikacija dejavnosti 2008. Dostopno na: https://www.stat.si/doc/pub/skd.pdf, http://www.stat.si/doc/klasif/SKD2008-Pojasnila-Klasje-SL.pdf.

[90] Statistični Urad RS (SURS). Dostopno na: http://www.stat.si/.

[91] Strategija kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti; februar 2016. Dostopno na: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/DSI2020_Strategija_Kibernetske_Varnosti.pdf.

[92] The 10 “must-haves” for secure enterprise mobility - A security framework and evaluators’ checklist; White Paper; Citrix, 2013. Dostopno na: https://www.citrix.com/content/dam/citrix/en_us/documents/oth/whitepaper-the-ten-must-haves.pdf.

[93] The Dzone Guide To Application Security, 2015 Edition, 30 strani. Dostopno na: https://dzone.com/guides/application-security-2015-edition.

[94] The European Agenda on Security, 2015. Dostopno na: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

[95] The Security Content Automation Protocol (SCAP). Dostopno na: https://scap.nist.gov/revision/index.html.

[96] Upravljanje neprekinjenega poslovanja - Palsit.si. Dostopno na: https://www.palsit.com/slo/storitve.php?page=49.

[97] You Have Been Hacked! – Hold Security, LLC, October, 2014. Dostopno na: http://holdsecurity.com/news/cybervor-breach/.

[98] ZEGART, Amy: "Cyberwar", TEDxStanford, Objavljeno 9. junija 2015. Dostopno na: http://fsi.stanford.edu/people/amy_zegart, https://www.youtube.com/watch?v=JSWPoeBLFyQ&feature=youtu.be&t=213